

IGEL Universal Management Suite v4

Benutzerhandbuch

UMS4

Universal Management Suite

Wichtige Informationen

Beachten Sie einige wichtige Informationen, bevor Sie dieses Handbuch lesen.

Copyright

Warenzeichen

IGEL ist ein eingetragenes Markenzeichen der IGEL Technology GmbH.

Alle anderen in diesem Handbuch genannten Namen oder Produkte können eingetragene Warenzeichen der entsprechenden Unternehmen oder durch diese urheberrechtlich geschützt sein und werden nur zur Erklärung oder Kennzeichnung und zum Vorteil des Eigentümers angegeben.

Haftungsausschluss

Die in diesem Handbuch enthaltenen Spezifikationen und Informationen dienen lediglich der Information, unterliegen zu jedem Zeitpunkt dem Recht auf Änderung ohne Ankündigung und stellen keine Verpflichtung der IGEL Technology GmbH dar. Die IGEL Technology GmbH übernimmt keine Verantwortung oder Haftung für eventuell in diesem Handbuch enthaltene Fehler oder Ungenauigkeiten; einschließlich in Bezug auf die hierin beschriebenen Produkte und Software-Programme. Die IGEL Technology GmbH übernimmt keine Gewährleistungen oder Garantien bezüglich des Inhalts dieses Dokuments und schließt insbesondere jede implizierte Garantie bezüglich der Marktgängigkeit und der Eignung für einen bestimmten Zweck aus.

IGEL Support und Knowledge Base

Wenn Sie bereits IGEL-Kunde sind, wenden Sie sich bitte zunächst an den für Sie zuständigen Vertriebspartner. Er beantwortet gerne Ihre Fragen rund um alle IGEL-Produkte.

Wenn Sie zur Zeit IGEL Produkte testen, oder falls Sie von Ihrem Vertriebspartner die gewünschte Hilfe nicht bekommen können, verwenden Sie bitte das IGEL Support Formular auf der Seite http://www.igel.com/de/mitgliederbereich/anmelden-abmelden.html .

Wir werden Sie umgehend unterstützen. Sie erleichtern die Arbeit unserer Support-Mitarbeiter, wenn Sie uns möglichst alle verfügbaren Informationen zukommen lassen. Bitte beachten Sie hierzu auch unsere *Hinweise zu Support- und Serviceauskünften http://www.igel.com/de/unternehmen/rechtliche-hinweise/support-und-serviceauskuenfte.html*.

Besuchen Sie die *IGEL Knowledge Base http://edocs.igel.com/*. Dort finden Sie neben den Benutzerhandbüchern auch ergänzende Dokumentation in Form von Best Practice oder How-to sowie die IGEL Support-FAQ.

Inhaltsverzeichnis

1. IGEL Universal Management Suite 8
1.1. Typische Einsatzbereiche 8
1.2. Eigenschaften der IGEL UMS 9
1.3. Komponenten der IGEL UMS 10
2. Installation 12
2.1. Installationsvoraussetzungen 12
2.2. Installation eines UMS-Servers 13
2.3. UMS-Installation aktualisieren 15
2.4. Anbindung externer Datenbanksysteme 17
3. Erste Schritte 19
3.1. UMS-Konsole mit Server verbinden 19
3.2. Thin Clients am UMS Server registrieren 21
4. Arbeiten mit IGEL UMS 28
4.1. Das Konsolenfenster 28
4.2. Der IGEL UMS-Administrator 39
5. Thin Clients 46
5.1. Thin Clients verwalten 46
5.2. Thin Clients konfigurieren 52
5.3. Spiegeln (VNC) 53
5.4. Firmware Lizenzen 59
6. Profile 62
6.1. Rangfolge der Einstellungen 63
6.2. Rangfolge der Profile 63
6.3. Profile verwenden 64
6.4. Benutzerprofile - IGEL Shared Workplace 71
6.5. Masterprofile 78
6.6. Templateprofile 83
7. Views 96
7.1. Neue View erstellen 96
7.2. View Ergebnisliste speichern 101
7.3. View per E-Mail verschicken 102
8. Geplante Aufgaben 103
8.1. Neue Aufgabe anlegen 103
8.2. Kommandos für Aufgaben 104
8.3. Details 105
8.4. Zeitplan 106
8.5. Zuordnung 107
8.6. Ergebnisse 107

9. Dateien ... 109
9.1. Datei am UMS Server registrieren ... 109
9.2. Datei zum Thin Client übertragen ... 110
9.3. Datei vom Thin Client entfernen ... 111
9.4. Datei auf den UMS Server übertragen ... 111
10. Universal Firmware Update ... 112
10.1. Servereinstellungen ändern ... 112
10.2. Update suchen und herunterladen ... 113
10.3. Von lokaler Quelle importieren ... 114
10.4. Aus dem UMS WebDAV importieren ... 114
10.5. Update einem Thin Client zuweisen ... 115
11. Zertifikate verwalten ... 116
11.1. Installation von Serverzertifikaten ... 116
11.2. Zertifikat entfernen ... 116
11.3. Zertifikat speichern ... 116
11.4. Konsolenzertifikat importieren ... 117
12. Administrationsbereich ... 117
12.1. UMS Netzwerk ... 117
12.2. UMS-Server ... 118
12.3. Globale Konfiguration ... 119
13. Active Directory Benutzer importieren ... 127
13.1. Symbolerklärung ... 129
13.2. Suche im Active Directory ... 129
13.3. Ergebnisliste des Imports ... 130
14. Administratorkonten und Zugriffsrechte ... 131
14.1. Administratoren und Gruppen ... 131
14.2. Zugriffsrechte ... 132
15. Benutzerprotokolle ... 139
15.1. Administration ... 139
15.2. Dialogfenster Logging ... 140
16. Logdateien und Support ... 143
17. Optionale Erweiterungen (HA und UCB) ... 143
17.1. IGEL UMS High Availability (HA) ... 143
17.2. IGEL Universal Customization Builder (UCB) ... 152
18. Glossar ... 162
19. Index ... 163

Über dieses Dokument

In diesem Dokument wird die Installation und Handhabung der IGEL Universal Management Suite (UMS) basierend auf Version 4.09.100 beschrieben. Die Firmware-Parameter des Thin Clients sind im jeweiligen Handbuch zu IGEL Universal Desktop oder IGEL Zero detaillierter beschrieben, auch wenn sich diese Parameter über die UMS konfigurieren lassen.

In diesem Dokument wird vorausgesetzt, dass eine funktionierende Installation der IGEL UMS sowie mindestens ein zu verwaltender IGEL-Thin Client vorhanden sind.

IGEL one-Thin Clients können in der UMS zwar registriert, jedoch nicht konfiguriert werden.

Dieses Handbuch ist in folgende Abschnitte unterteilt:

IGEL Universal Management Suite (Seite 8)	Eigenschaften und Komponenten der UMS
Installation (Seite 12)	Voraussetzungen, Installation, Update, externe DB-Systeme
Erste Schritte (Seite 19)	Verbindung zum Server herstellen, registrieren
Arbeiten mit IGEL UMS (Seite 28)	Konsolenfenster und Administrator
Thin Clients (Seite 46)	verwalten, konfigurieren, spiegeln; Firmwarelizenzen
Profile (Seite 62)	erstellen, konfigurieren; Benutzerprofile (IGEL Shared Workplace)
Views (Seite 96)	erstellen, speichern
Geplante Aufgaben (Seite 103)	anlegen, Details, Zeitplan, Zuordnung, Ergebnisse
Dateien (Seite 109)	am Server und Client registrieren, übertragen und entfernen
Universal Firmware Update (Seite 112)	vorbereiten, suchen, herunterladen, importieren, zuweisen
Zertifikate verwalten (Seite 116)	Installation von Server- und Konsolenzertifikaten
Administrationsbereich (Seite 117)	UMS-Server, Globale Konfiguration
Active Directory Benutzer importieren (Seite 127)	Symbole, Suche im AD, Ergebnisliste des Imports
Administratorkonten und Zugriffsrechte (Seite 131)	Administratoren, Gruppen, Berechtigungen
Benutzerprotokolle (Seite 139)	allgemein, Administration, Logging, Filtereinstellungen
Logdateien und Support (Seite 143)	Hilfestellungen
Anhang (Seite 143)	UMS High Availability Extension, Universal Customization Builder

Was ist neu in 4.09.100?

Die Release Notes der IGEL Universal Management Suite 4.09.100 finden Sie sowohl als Textdatei neben den Installationsprogrammen auf unserem *Downloadserver* (*http://myigel.biz/index.php?dir=IGEL_UNIVERSAL_MANAGEMENT_SUITE/*), als auch innerhalb unserer *Knowledge Base* (*http://edocs.igel.com/*).

Die wichtigste funktionale Änderung in dieser Version ist das Konzept der *Masterprofile* (Seite 78), welches die Konfiguration der Thin Clients durch besser steuerbare Administratorrechte noch flexibler und übersichtlicher gestaltet.

Daneben kann die IGEL Universal Management Suite nun *Views per E-Mail verschicken* (Seite 102) - fallweise auf Klick oder automatisiert per *Administrativer Aufgabe* (Seite 121).

UMS bietet nun die Möglichkeit, für die Kommunikation mit dem Server *ausschließlich per HTTPS (SSL)* (Seite 40) gesicherte Verbindungen zu erlauben.

Die verwendete Java-Version wurde aktualisiert. Um die UMS-Konsole per Java Web Start aufzurufen ist nun Java 1.8.0_40 oder neuer erforderlich.

1. IGEL Universal Management Suite

Die IGEL Universal Management Suite (UMS) ist eine benutzerfreundliche und äußerst effiziente Software, mit der IGEL-Thin Clients remote konfiguriert und gesteuert werden können. Durch den Einsatz der UMS werden die Kosten für Administration und Support der Arbeitsplätze verringert. Aufgrund der offenen und netzwerkfreundlichen Struktur lässt sie sich in die bestehende Unternehmensinfrastruktur optimal einbinden.

Die IGEL Universal Management Suite setzt neue Maßstäbe in der Verwaltung moderner Thin Clients. Sie bietet ein breites Spektrum an Merkmalen, die die Verwaltung von großen Thin Client-Umgebungen mit unterschiedlichen Konfigurationen auch über WANs hinweg schnell, einfach und sicher machen. Dank der Unterstützung unterschiedlichster Betriebssysteme, Datenbanken und Verzeichnisdienste wie Microsoft® Active Directory lässt sich die Universal Management Suite einfach in jede bestehende Umgebung einbinden.

Im Lieferumfang jedes IGEL-Thin Clients ist jeweils eine kostenlose Version der IGEL Universal Management Suite enthalten. In Kombination mit der herausragenden IGEL-Hardware erhalten Sie damit die fortschrittlichste Thin Client-Lösung, die der Markt derzeit zu bieten hat.

Eine Übersicht über die von der IGEL Universal Management Suite unterstützten Geräte finden Sie *in dieser FAQ http://edocs.igel.com/index.htm#10202898.htm*.

1.1. Typische Einsatzbereiche

- Automatische Einrichtung von Thin Clients mit der richtigen Konfiguration bei Inbetriebnahme
- Einstellungsänderungen der Geräte sowie der Software-Clients, Tools und lokalen Protokolle
- Verteilung von Updates und Firmware Images
- Diagnose und Support

1.2. Eigenschaften der IGEL UMS

Schnelle Installation:	Ein Assistent hilft Ihnen bei der Installation. Optional zur integrierten Datenbank können externe Datenbanksysteme angebunden werden.
Einfache Verwaltung per Mausklick:	Die meisten Hardware- bzw. Softwareeinstellungen können mit wenigen Klicks vorgenommen werden.
Einheitliche Benutzeroberfläche:	Die UMS-Benutzeroberfläche gleicht der lokalen Thin Client-Konfiguration. Die zusätzlichen Remote Management-Funktionen ermöglichen dem Administrator volle Kontrolle in gewohnter und bewährter Umgebung.
Kein Scripting:	Obwohl Scripting unterstützt wird, wird es nur im absoluten Ausnahmefall für die Steuerung der Thin Client-Konfiguration benötigt.
Asset Management:	Automatische Erfassung sämtlicher Hardwareinformationen, lizenzierter Features und installierter Hotfixes.
Kommentarfelder:	Für verschiedene kundenspezifische Informationen wie Standort, Installationsdatum oder Inventarnummer.
Unterstützung zahlreicher Betriebssysteme:	Der UMS-Server kann auf vielen gängigen Versionen von Microsoft® Windows®-Server und Linux ausgeführt werden, siehe Installationsvoraussetzungen.
Betriebssystem-unabhängiger Zugriff:	Die UMS-Konsole arbeitet Java-basiert und ermöglicht eine Systemverwaltung über jedes Gerät mit Java Runtime Environment – auch ohne lokale Installation der UMS-Konsole (Java Web Start), siehe *Installationsvoraussetzungen* (Seite 147).
Verschlüsselte Kommunikation:	Zertifikatsbasierte, SSL-verschlüsselte Kommunikation zwischen Remote Management-Servern und Clients für den Schutz vor nicht berechtigter Neukonfiguration der Geräte.
Ausfallsichere Update-Funktion:	Im Falle eines Ausfalls des Thin Clients während des Update-Prozesses - z. B. durch Stromausfall oder Verlust der Netzwerkverbindung - bleibt das Gerät funktionsfähig. Der Update-Vorgang wird beim nächsten Start abgeschlossen.
Basiert auf Standard-Kommunikations-Protokolle:	Eine Neukonfiguration der Router und Firewalls ist aufgrund der Nutzung von HTTP und FTP nicht erforderlich.
Unterstützung umfassender Umgebungen:	Die IGEL Universal Management Suite ist auf mehrere tausend Thin Clients skalierbar.
Gruppen- und profilbasierte Verwaltung:	Thin Clients innerhalb einer Organisationseinheit können ganz einfach über Profile verwaltet werden. Wechseln Mitarbeiter in eine andere Abteilung, kann der Administrator die neuen Einstellungen problemlos per Drag-and-Drop vornehmen.
Problemloser Roll-out:	IGEL-Thin Clients können auf Basis des jeweiligen Subnetzes bzw. basierend auf einer durch IGEL bereitgestellten MAC-Adressenliste automatisch einer Gruppe zugeordnet werden und erhalten automatisch die an die Gruppe gebundenen Konfigurationseinstellungen.

Umfassende Unterstützung aller Konfigurationsparameter:	Die Steuerung der meisten IGEL Thin Client-Einstellungen wie z. B. die Geräte- oder Sitzungskonfiguration erfolgt mithilfe der per Mausklick bedienbaren UMS-Benutzeroberfläche.
Übertragung von administrativen Rechten:	Große Organisationen können mehrere Systemadministratoren für jeweils unterschiedliche Steuerungs- und Berechtigungsbereiche bevollmächtigen. Diese administrativen Konten können aus einem Active Directory importiert werden.
Planung von Aufgaben:	Wartungsaufgaben können für die Nachtstunden eingeplant werden, sodass der tägliche Betrieb nicht beeinträchtigt wird.
VNC Shadowing:	Das IT-Support-Team kann remote auf die Bildschirme der Thin Clients zugreifen, um Probleme zügig zu identifizieren und dem Benutzer die Lösung direkt zu demonstrieren.

1.3. Komponenten der IGEL UMS

Das Programm IGEL Universal Management Suite - im Folgenden als UMS bezeichnet - besteht aus den drei Komponenten:

- IGEL UMS-*Server* (Seite 10)
- IGEL UMS-*Administrator* (Seite 11)
- IGEL UMS-*Konsole* (Seite 11)

1.3.1. UMS-Server – Das Back-End

Der UMS-Server ist eine Serveranwendung, für die ein relationales Datenbankmanagement-System (RDBMS), i. F. Datenbank, erforderlich ist; siehe *Installationsvoraussetzungen* (Seite 147) für unterstützte Datenbanken. Die Datenbank kann sowohl auf dem Server selbst, als auch auf Remote Hosts installiert und angebunden werden.

Der IGEL UMS-Server kommuniziert intern mit der Datenbank und extern mit den registrierten Thin Clients sowie mit der "Steuerzentrale", der UMS-Konsole:

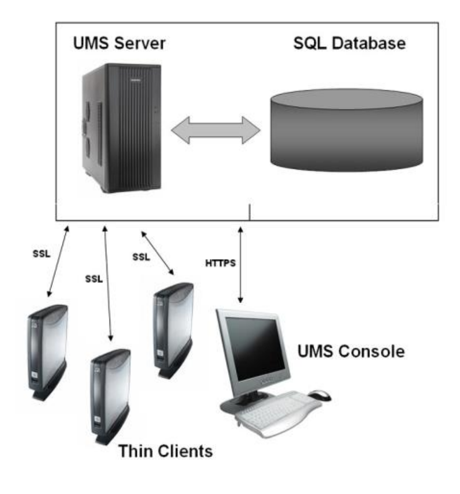


Abbildung 1: Das Backend

Die Datenübertragung zwischen Server und Thin Clients bzw. Konsole ist verschlüsselt. Typischerweise ist die UMS-Konsole auch auf anderen Rechnern im Netzwerk installiert als auf dem Serversystem. Die Kommunikation des UMS-Servers mit der Konsole, der Datenbank und den Thin Clients ist im Anhang näher beschrieben.

Jede Konfiguration der verwalteten Thin Clients wird in der Datenbank gespeichert. Änderungen in der Konfiguration werden in der Datenbank vorgenommen und bei Bedarf an den Thin Client übertragen. Der Thin Client kann die Informationen beim Startvorgang aus der Datenbank abrufen oder Sie können die neue Konfiguration manuell an den Thin Client senden. Ein zeitgesteuertes Konfigurationsupdate ist ebenfalls möglich.

1.3.2. UMS-Administrator – Das Verwaltungsprogramm

Der UMS-Administrator ist eine Verwaltungskomponente des UMS-Servers und nur dort verfügbar.

Zentrale Bestandteile des UMS-Administrators sind:

- Netzwerkkonfiguration (Ports, WebDAV-Ressourcen)
- Datenbankkonfiguration (Datenquellen, Backups)

Viele Administrationsaufgaben stehen auch über die UMS-Konsole zur Verfügung.

1.3.3. UMS-Konsole – Die zentrale Schaltstelle

Die UMS-Konsole ist die Schnittstelle zum UMS-Server.

Zentrale Aufgaben der UMS-Konsole sind:

- Darstellung der Konfigurationsparameter der Thin Clients
- Einrichtung von Profilen und geplanten Aufgaben
- Verwaltung von Firmware Updates

Die Verwaltung der Thin Clients und deren Konfiguration erfolgt über die GUI der UMS-Konsole. Sie ist die zentrale Schaltstelle der Thin Client-Administration. Die Konsole kann entweder am Server selbst oder lokal auf einem anderen Rechner im Netzwerk installiert sein oder auch als Java Web Start-Anwendung ohne Installation gestartet werden.

2. Installation

In diesem Kapitel erfahren Sie, welche Voraussetzungen gegeben sein müssen, um die UMS erfolgreich installieren zu können. An einem Beispiel zeigen wir Ihnen eine Installation mit *Windows* (Seite 13)-oder *Linux* (Seite 14)-Betriebssystem. Weiterhin erfahren Sie, was Sie bei einem Update beachten müssen und wo Sie externe Datenbanksysteme anbinden.

2.1. Installationsvoraussetzungen

Um IGEL Universal Management Suite installieren zu können, müssen folgende Mindestanforderungen an Hard- und Software erfüllt sein:

UMS-Komplettinstallation

- Mind. 1 GB RAM, 2 GB empfohlen
- Mind. 1 GB freier HDD-Speicher (Zzgl. Datenbanksystem)
- Die unterstützten Betriebssysteme entnehmen Sie bitte dem UMS-Datenblatt auf der IGEL-Webseite.

Tipp: *FAQ zur Installation von UMS auf 64-Bit-Systemen* (*http://edocs.igel.com/#10201860.htm*)

Einzelne Konsoleninstallation

- Mind. 512-MB-RAM, 1 GB empfohlen
- Mind. 250-MB-HDD-Speicher
- Java Web Start-Konsole: Java 1.8.0_40 oder neuer erforderlich
- Die unterstützten Betriebssysteme entnehmen Sie bitte dem UMS-Datenblatt auf der IGEL-Webseite.

Warnung: UMS-Server darf nicht auf einem Domain-Controller-System installiert werden. Die manuelle Änderung des Java Runtime Environment auf dem UMS-Server wird nicht empfohlen. Der Betrieb zusätzlicher Apache Tomcat-Webserver zusammen mit dem UMS-Server wird ebenfalls nicht empfohlen.

Die unterstützten Datenbanksysteme finden Sie im UMS-Datenblatt auf der IGEL-Webseite. Die Installations- und Betriebsvoraussetzungen für die Datenbank finden Sie in der Dokumentation des jeweiligen DBMS.

UMS-Server und Load Balancer für Hochverfügbarkeit (*High Availabilty* (Seite 143), HA) müssen IP-technisch im gleichen Netz stehen, ohne NAT oder Proxys, welche die Kommunikation der Komponenten beeinflussen.

Die interne Datenbank (Embedded-DB) kann **nicht** für ein HA -Netzwerk verwendet werden. Für eine reine Testinstallation mit nur einem einzigen Server für UMS-Server und Load Balancer können Sie auch die Embedded-Datenbank verwenden. Ein echtes HA-Netzwerk lässt sich damit jedoch nicht aufbauen.

2.2. Installation eines UMS–Servers

In diesem Beispiel wird die vollständige Installation eines UMS-Servers mit interner Embedded-DB beschrieben. Bei abweichenden Installationen wählen Sie die entsprechenden Komponenten einzeln aus - z. B. für eine einzelne Konsoleninstallation.

> Die Installationsanweisung für die UMS-HA (High Availability)-Extension finden Sie im *Anhang* (Seite 143).

2.2.1. Unter WINDOWS installieren

So installieren Sie die IGEL Universal Management Suite unter Windows:

1. Laden Sie sich zunächst die aktuelle Version der IGEL Universal Management Suite vom IGEL-Downloadserver herunter und starten Sie den Installer durch Ausführen der `EXE`–Datei.

   > Sie benötigen Administrationsrechte auf dem Rechner, um IGEL UMS installieren zu können.

2. Schließen Sie andere Anwendungen und bestätigen Sie dies.
3. Lesen und bestätigen Sie die Lizenzvereinbarung.
4. Lesen Sie die Erläuterung des Installationsprozesses.
5. Wählen Sie einen Pfad für die Installation.
6. Wählen Sie den Installationsumfang (s.o.).
7. Setzen Sie einen Benutzer und das Passwort für die Datenbankverbindung.
8. Wählen Sie einen Namen für den Eintrag im Windows-Startmenü.
9. Lesen Sie die Zusammenfassung und starten Sie den Prozess.
10. Schließen Sie das Programm nach Abschluss der Installation.

    Haben Sie die Standardinstallation gewählt, läuft nun der IGEL Universal Management Suite-Server mit der Embedded-Datenbank.

11. Starten Sie die UMS-Konsole.
12. Verbinden Sie sich zum Server mit den Zugangsdaten, die bei der Installation angegeben wurden (Datenbankbenutzer).

    > Zur Verwendung von UMS mit externen Datenbanken siehe *Anbindung externer Datenbanken* (Seite 17).

Der Windows-Installer erstellt Einträge im Windows-Softwareverzeichnis und im Startmenü. Ein Icon zum Start der UMS-Konsole wird auf dem Desktop abgelegt.

> Tipp: *FAQ zur Installation von UMS auf 64-Bit-Systemen* (*http://edocs.igel.com/#10201860.htm*)

2.2.2. Unter LINUX installieren

So installieren Sie die IGEL Universal Management Suite unter LINUX:

1. Laden Sie sich zunächst die aktuelle Version der IGEL Universal Management Suite vom IGEL-Downloadserver herunter. Das Installationsprogramm unter Linux ist eine X11-Anwendung.
2. Loggen Sie sich als `ROOT` ein.

   > Sie benötigen `ROOT`-Rechte auf dem Rechner, um die IGEL UMS installieren zu können.

3. Öffnen Sie ein Terminal-Fenster wie xterm, Konsole, Gnome-Terminal usw. und wechseln Sie in das Verzeichnis des Installationspakets.
4. Prüfen Sie das Paket auf Ausführbarkeit, ggf. müssen Sie diese erst erstellen mit

   ```
   chmod a+x setup*.bin.
   ```

5. Führen Sie die Installationsdatei `setup-igel-ums-linux-0.1.bin` aus. Verwenden Sie ggf. `sudo`, um mit `ROOT`-Rechten auszuführen.

   Der Installer entpackt sich nach /`tmp`, führt seine Java Engine aus und entfernt sich nach Abschluss der Installation wieder selbst.

6. Schließen Sie andere Anwendungen und bestätigen Sie dies.
7. Lesen und bestätigen Sie die Lizenzvereinbarung.
8. Lesen Sie die Erläuterung des Installationsprozesses.
9. Wählen Sie einen Pfad für die Installation.
10. Wählen Sie den Installationsumfang (s.o.).
11. Setzen Sie einen Benutzer und das Passwort für die Datenbankverbindung.
12. Lesen Sie die Zusammenfassung und starten Sie den Prozess.
13. Schließen Sie das Programm nach Abschluss der Installation.

    Haben Sie die Standardinstallation gewählt, läuft nun der IGEL Universal Management Suite-Server mit der Embedded-Datenbank.

14. Starten Sie die UMS-Konsole im Installationsverzeichnis, z.B. `/opt/IGEL/RemoteManager/RemoteManager.sh`
15. Verbinden Sie sich zum Server mit den Zugangsdaten, die Sie bei der Installation angegeben haben.

    > Zur Verwendung von UMS mit externen Datenbanken siehe *Anbindung externer Datenbanken* (Seite 17).

> Tipp: *FAQ zur Installation von UMS auf 64-Bit-Systemen* (*http://edocs.igel.com/#10201860.htm*)

2.3. UMS–Installation aktualisieren

Erstellen Sie ein Backup der Datenbank, bevor Sie eine zuvor installierte Version der IGEL UMS aktualisieren.

Sollten Sie noch eine ältere Version des IGEL Remote Managers mit SAP DB verwenden, so empfehlen wir den Umzug auf die Embedded-DB bevor Sie die IGEL UMS aktualisieren. Wenden Sie sich für eine nähere Beschreibung dieses Umzugs bitte an den IGEL-Support.

> **Warnung:** Die Installation einer älteren als der aktuell verwendeten UMS-Version ist nur möglich, wenn Sie ein Backup der Datenbank mit dem passenden älteren Schema haben. Denn die Aktualisierung des Datenbankschemas funktioniert nur auf neuere Versionen und kann nicht rückgängig gemacht werden! Um diesen Rückweg zur Vorversion zu gewährleisten, sollten Sie vor Aktualisierung der UMS von Ihrem laufenden System Backups anfertigen.

Die Einrichtung eines Testsystems ist zu empfehlen, um neue Versionen der IGEL UMS zunächst dort zu installieren und erst nach Überprüfung Ihrer Prozesse in das Produktivsystem zu übernehmen. Dies trifft auch für Hotfixes, Patches etc. von Serversystem und Datenbank zu.

> Mit einer Konsolenversion, die älter ist als die Version des Servers, können Sie sich nicht zum Server verbinden (Fehlermeldung `Unable to load tree`). Aktualisieren Sie in diesem Fall auch die Konsoleninstallation.

2.3.1. Unter WINDOWS aktualisieren

So führen Sie ein Update unter Windows aus:

1. Laden Sie sich zunächst die aktuelle Version der IGEL Universal Management Suite vom IGEL-Downloadserver herunter und starten Sie den Installer durch Ausführen der `EXE`–Datei.

   > Sie benötigen Administrationsrechte auf dem Rechner, um die IGEL UMS installieren zu können.

2. Schließen Sie andere Anwendungen und bestätigen Sie dies.
3. Lesen und bestätigen Sie die Lizenzvereinbarung.
4. Lesen Sie die Erläuterung des Installationsprozesses.
5. Wählen Sie einen Pfad für die Installation.
6. Wählen Sie einen Namen für den Eintrag im Windows-Startmenü.
7. Lesen Sie die Zusammenfassung und starten Sie den Prozess.
8. Bestätigen Sie, dass alle anderen UMS-Anwendungen beendet wurden.
9. Bestätigen Sie die automatische Aktualisierung des Datenbankschemas (s. Warnung oben).
10. Schließen Sie das Programm nach Abschluss der Installation.

Nach erfolgreicher Update-Installation verbindet sich der UMS-Server wieder mit der zuvor verwendeten Datenbank.

11. Starten Sie die UMS-Konsole und verbinden Sie sich zum Server mit den Zugangsdaten, die Sie bei der Installation angegeben haben.

Der Windows-Installer erstellt Einträge im Windows-Softwareverzeichnis und im Startmenü. Ein Icon zum Start der UMS-Konsole wird auf dem Desktop abgelegt.

2.3.2. Unter LINUX aktualisieren

So führen Sie ein Update unter Linux aus:

1. Laden Sie sich zunächst die aktuelle Version der IGEL Universal Management Suite vom IGEL-Downloadserver herunter. Das Installationsprogramm unter Linux ist eine X11-Anwendung.
2. Loggen Sie sich als `ROOT` ein.

   > Sie benötigen `ROOT`-Rechte auf dem Rechner, um die IGEL UMS installieren zu können.

3. Öffnen Sie ein Terminal-Fenster wie xterm, Konsole, Gnome-Terminal usw. und wechseln Sie in das Verzeichnis des Installationspakets.
4. Prüfen Sie das Paket auf Ausführbarkeit, ggf. müssen Sie diese erst erstellen mit

   `chmod a+x setup*.bin.`

5. Führen Sie die Installationsdatei `setup-igel-ums-linux-0.1.bin` aus. Verwenden Sie ggf. `sudo`, um mit `ROOT`-Rechten auszuführen.

   Der Installer entpackt sich nach `/tmp`, führt seine Java Engine aus uns entfernt sich nach Abschluss der Installation wieder selbst.

6. Schließen Sie andere Anwendungen und bestätigen Sie dies.
7. Lesen und bestätigen Sie die Lizenzvereinbarung.
8. Lesen Sie die Erläuterung des Installationsprozesses.
9. Wählen Sie einen Pfad für die Installation.
10. Lesen Sie die Zusammenfassung und starten Sie den Prozess.
11. Bestätigen Sie, dass alle anderen UMS-Anwendungen beendet wurden.
12. Bestätigen Sie die automatische Aktualisierung des Datenbankschemas (s. Warnung oben).
13. Schließen Sie das Programm nach Abschluss der Installation.

    Nach erfolgreicher Update-Installation verbindet sich der UMS-Server wieder mit der zuvor verwendeten Datenbank.

14. Starten Sie die UMS-Konsole im Installationsverzeichnis, z.B. `/opt/IGEL/RemoteManager/RemoteManager.sh`
15. Verbinden Sie sich zum Server mit den Zugangsdaten, die Sie bei der Installation angegeben haben.

2.4. Anbindung externer Datenbanksysteme

Die unterstützten Datenbanksysteme finden Sie im Datenblatt der IGEL UMS bzw. der HA-Erweiterung auf der IGEL-Webseite. Die Installations- und Betriebsvoraussetzungen für die Datenbank finden Sie im Administrationshandbuch des jeweiligen DBMS.

➢ Konfigurieren Sie die Datenbank im jeweiligen Verwaltungsprogramm des DBMS.

Die Erstellung der Datenquelle und Anbindung der UMS an die Datenbank konfigurieren Sie im UMS-Administrator.

> Alle UMS-Server müssen mit der selben Datenbank arbeiten.

2.4.1. Oracle

So binden Sie Oracle an:

1. Erstellen Sie einen neuen Datenbankbenutzer mit `Ressource`–Berechtigung.
2. Legen Sie im UMS-Administrator eine neue Datenquelle vom Typ Oracle an.

> Einige Oracle-Versionen legen die Rolle `Ressource` ohne `CREATE VIEW`–Berechtigung an, stellen Sie sicher, dass diese Berechtigung in der Rolle gesetzt ist.

2.4.2. Microsoft SQL Server

So binden Sie Microsoft SQL Server an:

1. Öffnen Sie die SQL-Konsole des SQL-Servers über **New Query**.
2. Verwenden Sie das folgende Skript als Vorlage, passen Sie es an und führen Sie es aus.

   > Um Probleme bei der Aktivierung der Datenquelle zu vermeiden stellen Sie bitte sicher, dass `LOGIN`, `USER` und `SCHEMA` gleich benannt sind.

```
CREATE DATABASE rmdb
GO
USE rmdb
GO
CREATE LOGIN igelums with PASSWORD = 'setyourpasswordhere',
DEFAULT_DATABASE=rmdb
GO
CREATE USER igelums with DEFAULT_SCHEMA = igelums
GO
CREATE SCHEMA igelums AUTHORIZATION igelums GRANT CONTROL to igelums
GO
```

3. Legen Sie im UMS-Administrator eine neue Datenquelle vom Typ `SQL Server` an.
4. Stellen Sie sicher, dass der **Serverport** des SQL-Servers in der Datenquelle korrekt konfiguriert ist, der Standardwert ist `1433`.

   Der Microsoft-SQL-Server sollte **Windows- und SQL-Authentifizierung** zulassen.

2.4.3. PostgreSQL

So binden Sie PostgreSQL an:

Setzen Sie bei der Installation einer neuen Instanz der PostgreSQL-Datenbank folgende Parameter:

1. Installieren Sie das Datenbankcluster mit `UTF-8` **Kodierung.**
2. Akzeptieren Sie Verbindungen aller **Adressen**, nicht nur `localhost`.
3. Aktivieren Sie **Procedural Language** `PL/pgsql` in der Defaultdatenbank.

   Weitere Informationen zur Installation der PostgreSQL-Datenbank finden Sie unter http://www.postgresql.org.

Führen Sie nach der Installation folgende Konfigurationsschritte aus:

1. Ändern Sie die Serverparameter: In der Datei `postgresql.conf` muss der Parameter `listen_addresses` den Hostnamen des IGEL UMS-Server enthalten **ODER** `'*'`, um Verbindungen zu jedem Host zuzulassen.
2. Legen Sie in der Datei `pg_hba.conf` einen Parameter `host` an, um dem UMS-Server die Berechtigung für das Log-in mit den dort definierten Benutzerdaten zu geben.

   > Ist der IGEL UMS-Server auf derselben Maschine wie PostgreSQL-Server installiert, so sind keine Änderungen an diesen Dateien notwendig.

3. Starten Sie das Administrationstool pgAdmin.
4. Erstellen Sie eine neue Log-in-Rolle mit dem Namen `rmlogin`.
5. Erstellen Sie eine neue Datenbank mit

   name = `rmdb`
   owner = `rmlogin`
   encoding = `UTF-8`

6. Legen Sie ein neues Schema innerhalb der Datenbank rmdb an mit

   name = `rmlogin`

7. Prüfen Sie ob die Sprache plpgsql in der Datenbank rmdb besteht.

   Falls nicht, legen Sie diese an.

8. Legen Sie im **UMS-Administrator** eine neue Datenquelle vom Typ `PostgreSQL` an mit dem Hostnamen des PostgreSQL-Servers und dem korrekten Serverport (Vorgabe ist `5432`), Benutzer `rmlogin` und Datenbank `rmdb`.

2.4.4. Apache Derby

So binden Sie Apache Derby an:

Wie für die anderen externen Datenbanken empfehlen wir auch hier für die Verwendung durch IGEL UMS eine neue Datenbankinstanz anzulegen.

Führen Sie die folgenden Schritte aus, um eine neue Datenbankinstanz anzulegen und definieren Sie diese als Datenquelle im **UMS-Administrator**:

1. Aktivieren Sie zur Sicherheit **User Authentication** in der Derby-DB.
2. Starten Sie das ij Utility (in `[derby-installation-dir]/bin`).
3. Führen Sie folgendes Kommando aus, um die Instanz rmdb anzulegen:

```
connect
'jdbc:derby:rmdb;user=dbm;password=dbmpw;create=true';
```

4. Definieren Sie den UMS-Datenbankbenutzer `rmlogin` mit Passwort `rmpassword`

```
CALL SYSCS_UTIL.SYSCS_SET_DATABASE_PROPERTY('derby.user.rmlogin',
'rmpassword');
```

5. Verlassen Sie ij und starten Sie den Derby Network Server.
6. Legen Sie im **UMS-Administrator** eine neue Datenquelle vom Typ `Derby` an mit dem Hostnamen des Derby-Servers und dem korrekten Serverport (Vorgabe ist `1527`), Benutzer `rmlogin` und Datenbank `rmdb`.

   Weitere Informationen zur Installation der Derby-Datenbank finden Sie unter http://db.apache.org/derby.

3. Erste Schritte

Damit Sie mit der IGEL UMS arbeiten können, müssen Sie nach der Installation von UMS-Server, Konsole und Datenbank zumindest einen Thin Client registrieren oder das UMS-Demonstration Datenbank-Backup einspielen, dieses steht auf dem IGEL-Downloadserver zur Verfügung.

Im Folgenden wird beschrieben, wie Sie sich mit der UMS-Konsole zum Server verbinden und Thin Clients registrieren. Detaillierte Informationen zu den Funktionen der IGEL UMS finden Sie im Kapitel *Arbeiten mit IGEL UMS* (Seite 28).

3.1. UMS–Konsole mit Server verbinden

So stellen Sie eine Verbindung zum UMS-Server her:

1. Starten Sie die UMS-Konsole.
2. Klicken Sie **System→Verbinden mit...**, um sich sich mit dem UMS-Server zuverbinden.

3. Geben Sie die Server- und Benutzerdaten im Anmeldefenster ein:



Abbildung 2: Anmeldung an der Konsole

UMS-Server: Verwenden Sie den Hostnamen `localhost`, wenn Sie sich an der UMS-Konsole des Servers anmelden.

Verwenden Sie den Hostnamen des Servers, wenn Sie sich von einer entfernten UMS-Konsole verbinden.

Port: Der Port, auf dem der IGEL UMS-GUI-Server Verbindungen empfängt, ist standardmäßig auf `8443` gesetzt, kann jedoch mithilfe des Programms IGEL UMS Administrator geändert werden.

Benutzername und Passwort: Geben Sie den Benutzernamen und das Passwort eines UMS-Administrators ein. Bei Ersteinrichtung von IGEL UMS sind das die Informationen des Datenbank-Benutzerkontos, das während der Installation des UMS-Servers erstellt wurde. Melden Sie sich mit dem Benutzernamen `<Benutzer>@<Domäne>` an, wenn Sie einer im UMS konfigurierten Domäne angehören.

➢ Klicken Sie **Verbinden**.

Die hier eingegebenen Daten wie Servername, Port und Benutzername, werden für spätere Verbindungsvorgänge gespeichert. Beim nächsten Verbindungsaufbau müssen Sie lediglich das Passwort eingeben. Auch werden die zuletzt verwendeten Server- und Benutzerinformationen in Drop-down-Listen gespeichert und können so schnell wiederverwendet werden. Sie können diese Liste der gespeicherten Anmeldedaten löschen unter **Extras→Einstellungen→Allgemein→Login Historie löschen**.

3.2. Thin Clients am UMS Server registrieren

Die Aufnahme von Thin Clients in die UMS-Datenbank kann auf verschiedenen Wegen erfolgen:

- *Suche nach Thin Clients im Netzwerk* (Seite 21)
- *Import von Thin Clients über* `csv`*–Dateien* (Seite 24)
- *Manuelle Registrierung am Thin Client* (Seite 26)
- *Automatische Registrierung von Thin Clients* (Seite 27)
- *Manuelle Erstellung von Thin Clients* (Seite 27)

Falls Sie ein *eigenes Server-Zertifikat einspielen* (Seite 117) möchten, erledigen Sie das, bevor Sie Thin Clients an UMS registrieren. Ansonsten müssen Sie nach dem Zertifikatswechsel die alten Zertifikate manuell von den Thin Clients entfernen.

3.2.1. Thin Clients im Netzwerk suchen

So suchen Sie im Netzwerk nach Thin Clients und wählen Sie für die Registrierung aus:

1. Melden Sie sich an der UMS-Konsole an.

   Der Inhaltsbereich der Konsole wird angezeigt.

2. Klicken Sie **Thin Clients→Thin Clients scannen**, um zum Suchfenster für Thin Clients im Netzwerk zu gelangen.

   Alternativ starten Sie die Suche über die Schaltfläche der Symbolleiste.



Abbildung 3: Suche nach Thin Clients

3. Suchen Sie im gesamten Netzwerk nach eingeschalteten Thin Clients oder schränken Sie die Suche auf IP-Adressbereiche ein.

4. Wählen Sie die zu registrierenden Thin Clients in der Checkbox **Aufnehmen** aus.
5. Klicken Sie **OK**.

3.2.2. Thin Clients scannen

Ein Thin Client muss eingeschaltet und funktionsfähig sein, um gescannt werden zu können. Darüber hinaus muss die Firmware des Thin Clients die IGEL UMS-Software unterstützen. Dies ist bei allen IGEL-Thin Clients mit Originalfirmware der Fall, ebenso bei Geräten von Fremdherstellern, auf denen mittels IGEL Universal Desktop Converter 2 das IGEL Linux-System installiert wurde.

Folgende Scanoptionen stehen zur Verfügung:

Lokales Netzwerk des UMS-Servers	Bei dieser Option wird eine Broadcast-Nachricht durch das Netzwerk gesendet, in dem sich der IGEL UMS-Server befindet. Der IGEL UMS-Server kann sich in einem anderen Netzwerksegment als die IGEL UMS-Konsole befinden. Wenn der Server auf dem IGEL UMS-Server installiert ist und über verschiedene Netzwerkschnittstellen verfügt, wird nur die erste Schnittstelle verwendet, um die Broadcast-Nachricht zu senden.
IP-Bereich	Durch Versenden einer Nachricht wird jede IP im festgelegten Bereich kontaktiert, auch wenn Router Broadcast-Nachrichten unterdrücken.
Liste von IP-Bereichen	Wenn mehrere Netzwerksegmente gescannt werden müssen, können Sie eine Liste der IP-Bereiche einrichten. Klicken Sie dazu auf **Liste bearbeiten** und **Hinzufügen**, um Bereiche zu ergänzen.
TCP zum Suchen verwenden	Wählen Sie diese Option, um TCP statt UDP zum Scannen zu verwenden. Das Scannen mit TCP funktioniert in einigen Netzwerken zuverlässiger, dauert jedoch auch länger.

Nach Abschluss des Scanvorgangs werden die erkannten Thin Clients im Scanergebnisfenster in einer sortierbaren Liste angezeigt.

In der Spalte **Zertifikat gespeichert** können Sie sehen, ob ein Thin Client bereits über ein Zertifikat eines UMS-Servers verfügt. Thin Client-Zertifikate können jetzt am Server registriert werden.

Im Feld **Filter** können Sie einen Suchstring eingeben, z. B. Teile des Gerätenamens, der IP-Adresse oder der MAC-Adresse, der in allen sichtbaren Feldern gesucht wird.

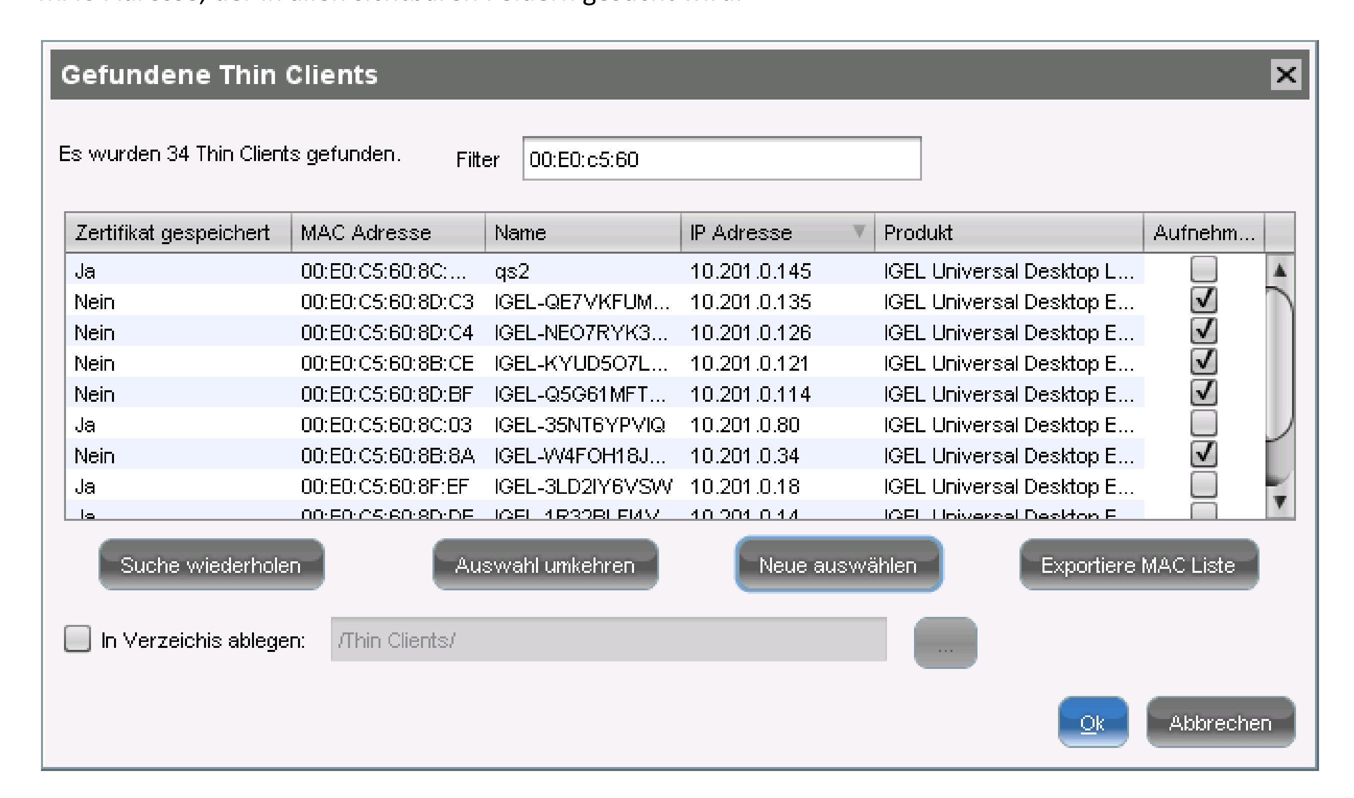


Abbildung 4: Ergebnisliste des Scanvorgangs

3.2.3. Thin Clients registrieren

So registrieren Sie neue Thin Clients:

1. Markieren Sie in der Spalte **Aufnehmen** die Thin Clients, die Sie in Ihrer IGEL UMS-Datenbank registrieren möchten.
2. Klicken Sie auf **Neue auswählen**, um alle Thin Clients ohne Zertifikat auszuwählen.
3. Bestätigen Sie Ihre Auswahl mit **OK**.

   Die Thin Clients werden in Ihrer Datenbank registriert. Dies kann je nach der Performance des IGEL UMS-Servers einige Zeit dauern.
   Wenn der Thin Client in der IGEL UMS-Datenbank registriert ist, wird das Serverzertifikat auf dem Thin Client gespeichert. Der weitere Zugriff auf den Thin Client wird nach diesem Zertifikat validiert. Nur der Eigentümer des anderen privaten Anteils des Zertifikats kann den Thin Client steuern.
4. Legen Sie die Thin Clients gleich bei der Registrierung in einem ausgewählten **Verzeichnis** des Navigationsbaums ab, so müssen Sie sie nicht manuell einsortieren.

   Das Ergebnis des Vorgangs und mögliche Fehlermeldungen werden in einem neuen Fenster angezeigt.
5. Schließen Sie diese Fenster, um zurück zum Hauptbildschirm zu gelangen.

3.2.4. Thin Clients importieren

Sie können Thin Clients bereits registrieren, bevor diese physikalisch im Netz installiert sind. Dazu brauchen Sie eine `csv`–Datei mit den für die Registrierung erforderlichen Informationen der Thin Clients. Das sind mindestens die MAC-Adresse, Thin Client-Name und Firmware-ID.

Die Firmware der Thin Clients muss für den Import bereits in der Datenbank vorhanden sein, entweder durch zuvor registrierte Thin Clients oder durch den Import der Firmware. Daher eignet sich diese Methode nur bedingt für die Ersteinrichtung von IGEL UMS.

1. Starten Sie unter **System→Importieren→Thin Clients importieren** den Import.

   Wenn ungültige Daten wie z. B. eine unbekannte Firmware oder ein Fehler während des Importvorgangs auftreten, wird eine entsprechende Meldung in der Nachrichtenanzeige im unteren Teil des Dialogfelds angezeigt. Die Zeile mit dem betreffenden Thin Client wird rot markiert.

2. Klicken Sie auf **Bereinigen**, um alle Meldungen aus der Anzeige zu löschen.

3. Klicken Sie **TCs importieren**, um den Importvorgang zu starten.

   Erfolgreich importierte Thin Clients werden grün markiert.

Das Dialogfenster **Import** beinhaltet einige einfache Bearbeitungsfunktionen, um letzte Änderungen vorzunehmen, z. B. um die Firmware-ID zu korrigieren:

- Strg-C und Strg-V zum Kopieren und Einfügen einer markierten Zeile
- Entf/Strg-X zum Löschen einer markierten Zeile
- Return/Eingabe fügt eine weitere Zeile unter einem Feld hinzu

Import mit kurzem Format

Das kurze Format liefert die für den Import notwendigen Informationen und die Zuordnung zu einem Profil: **MAC-Adresse, Gerätename, Firmware-ID, Profil-ID**.

> Die ID einer bereits registrierten Firmware finden Sie über **Extras→Firmwarestatistik**.
>
> Die ID einses Profils wird in den **Beschreibungsdaten** und im **Tooltip** des Profils angezeigt.

Beispiel:

```
00E0C5540B8B;IGEL-00E0C5540B8B;1;26
00E0C5540B8C;IGEL-00E0C5540B8C;1;26
00E0C5540B8D;IGEL-00E0C5540B8D;1;26
```

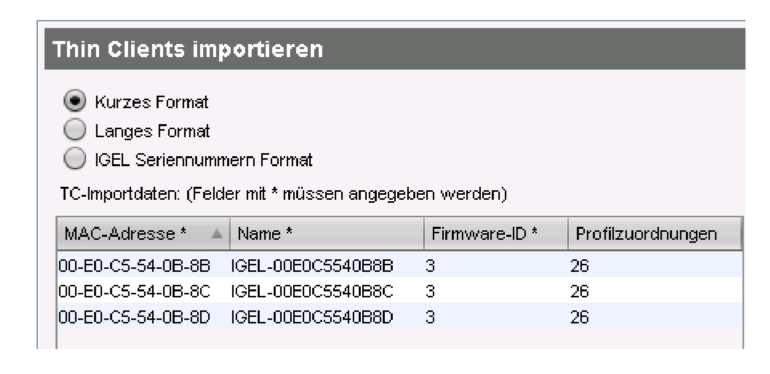


Abbildung 5: Import mit kurzem Format

Import mit langem Format

Das lange Format erlaubt im Unterschied zum Kurzformat auch den Import weiterer Daten wie Ablageverzeichnis im Navigationsbaum der UMS, Seriennummer, Standort u.a. Die importierbaren Informationen sehen Sie nach der Auswahl des Langformats im Importdialog.

Beispiel:

/Import;00E0C5540B9A;IGEL Universal Desktop LX;5.03.100.01;IGEL-1;Büro1;EDV;Meier;0815;01.06.2014;F44M;26;01

/Import;00E0C5540B9B;IGEL Universal Desktop LX;5.03.100.01;IGEL-2;Büro2;EDV;Müller;4711;01.06.2014;F45M;26;01

/Import;00E0C5540B9C;IGEL Universal Desktop LX;5.03.100.01;IGEL-2;Büro3;EDV;Schulz;42;01.06.2014;F46M;26;01

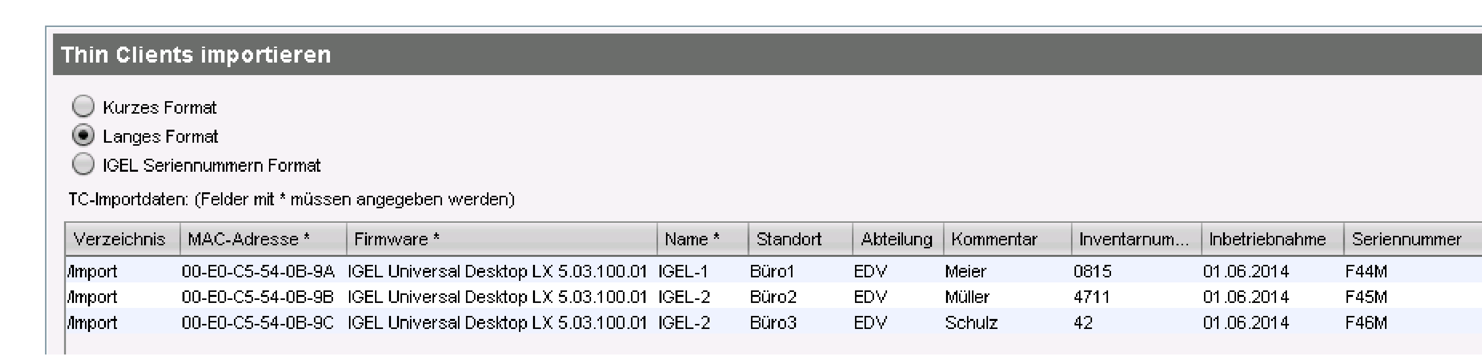


Abbildung 6: Import mit langem Format

Die Spalte **Firmware** der Vorschau wird zusammengesetzt aus zwei Werten der Importdatei (System und Version der Firmware).

Die ID einses Profils wird in den **Beschreibungsdaten** und im **Tooltip** des Profils angezeigt.

Import mit IGEL Seriennummer

Das **Seriennummernformat** erlaubt den Import der Thin Clients anhand einer zum Lieferauftrag erstellten Datei. Sie können diese Importdatei schon bei der Bestellung Ihrer IGEL Thin Clients anfordern, so lassen sich die Geräte bereits vor der Lieferung in die UMS integrieren und konfigurieren.

Beispiel:

```
08154711;14D3B8C01B14110EBE;00E0C56133E4
47110815;14D3B8C01B14110EC6;00E0C56133EC
42007ABC;14D3B8C01B14110ED7;00E0C56133FD
007ABC42;14D3B8C01B14110EF9;00E0C561341F
```



Abbildung 7: Import mit Seriennummernformat

Die Firmware des Geräts wird nicht aus der Datei importiert, als Vorgabe wird die Firmware mit der höchsten ID zugeordnet. Die IDs bereits registrierter Firmwares finden Sie über **Extras→Firmwarestatistik**.

Die Seriennummer steht in der Importdatei an erster Stelle jeder Zeile, in der Vorschau wird sie als letzte Spalte gelistet.

3.2.5. Thin Clients manuell registrieren

Sie können die Registrierung eines Thin Clients am UMS-Server auch am Client selbst vornehmen:

1. Tragen Sie im Setup des Thin Clients unter **System→Remote Management** den Namen bzw. die Adresse Ihres UMS-Servers und den Serverport ein (Standardeinstellung `30001`).
2. Führen Sie die Registrierung mit Angabe der Log-in-Daten des UMS-Servers durch.
3. Starten Sie den Thin Client neu.

Auf Thin Clients mit UDLX-Firmware finden Sie im **Starter für Anwendungen** unter **System** ein eigenes Programm zur Registrierung am UMS-Server. Damit können Sie vom Client aus das Unterverzeichnis des Navigationsbaums bestimmen, in welches der Client aufgenommen wird.

Es gibt zwei Möglichkeiten, dem Thin Client die IP-Adresse des UMS-Servers zu übermitteln:

- Wenn Sie einen Thin Client am UMS-Server registrieren, wird die IP-Adresse des Servers auf dem Thin Client gespeichert. Der Registry-Schlüssel ist: `system.remotemanager.server0.ip`.

  Der Thin Client verbindet sich mit dieser IP-Adresse, um bei jedem Bootvorgang seine Einstellungen abzurufen.
  Oder konfigurieren Sie Ihren DHCP-Server so, dass er über die Option 224 die IP-Adresse bekannt gibt.

- Die zweite Möglichkeit ist die Erstellung eines Alias mit dem Namen `igelrmserver` für den UMS-Server in Ihrem DNS.

Sie müssen eine dieser Möglichkeiten nutzen, wenn Sie manuell Thin Clients in Ihre UMS-Datenbank aufnehmen möchten. Anderenfalls kann der Thin Client sich nicht mit dem Server verbinden.

3.2.6. Thin Clients automatisch registrieren

Der IGEL UMS-Server lässt sich so konfigurieren, dass automatisch alle Thin Clients ohne Zertifikat registriert werden, die im Netzwerk des Servers hochfahren.

1. Aktivieren Sie dazu im Programm **IGEL UMS Administrator** unter **Einstellungen→Weitere Einstellungen** den Parameter **Automatisches Registrieren**.
2. Registrieren Sie einen IGEL-Thin Client automatisch am UMS-Server, indem Sie einen DNS-Eintrag `igelrmserver` (Record Type A) oder eine DHCP-Option (224) setzen.
3. Setzen Sie die DHCP-Option 224 als String - nicht als DWORD - auf die IP-Adresse des Servers, indem sie der Datei `dhcpd.conf` im entsprechenden Abschnitt, z. B. im globalen Bereich, folgendes hinzufügen:

   ```
   option igelrmserver code 224 = text
   option igelrmserver "<IP des UMS Servers>"
   ```

4. Setzen sie ebenfalls den DNS-Eintrag `igelrmserver` auf die IP-Adresse des UMS-Servers.

Warnung: Ist diese Option aktiviert, wird jeder Thin Client ohne Zertifikat im Netzwerk in die UMS-Datenbank aufgenommen. Wenn Sie einen Client auf die Werkseinstellungen zurücksetzen und neu starten, wird er sofort erneut auf dem Server registriert. Wir empfehlen die automatische Registrierung dann, wenn neue Clients beim Rollout im Netzwerk registriert werden müssen. Deaktivieren Sie nach dieser Registrierung die Option der automatischen Registrierung am UMS-Server.

3.2.7. Thin Clients manuell erstellen

So erzeugen Sie manuell einen Eintrag eines Thin Clients direkt in der Datenbank:

1. Wählen Sie **Neuer Thin Client** entweder im Kontextmenü eines Thin Client-Verzeichnisses oder im Menü unter **System→Neu**.
2. Geben Sie die MAC-Adresse, den Namen und die Firmware des Thin Clients an und wählen Sie optional ein Verzeichnis für den Client.

Die Firmware der Thin Clients muss für die manuelle Erstellung bereits in der Datenbank vorhanden sein, entweder durch zuvor registrierte Thin Clients oder durch Import der Firmware. Daher eignet sich diese Methode nur bedingt für die Ersteinrichtung der IGEL UMS.

4. Arbeiten mit IGEL UMS

Die IGEL Universal Management Suite stellt umfangreiche Verwaltungswerkzeuge für Ihre Thin Client-Infrastruktur zur Verfügung. Der Hauptteil der administrativen Aufgaben befindet sich in der UMS-Konsole. Einige Werkzeuge zur Serverkonfiguration stellt der UMS-Administrator zur Verfügung.

Die Programmoberfläche und die vorhandenen Werkzeuge werden im Folgenden detailliert dargestellt.

4.1. Das Konsolenfenster

Die UMS-Konsole beinhaltet verschiedene Werkzeuge und Informationsbereiche.

Zentrale Bestandteile sind:

- Navigationsbaum
- (Kontext-)Menü
- Inhaltsbereich

Dies sind die Fensterbestandteile der UMS-Konsole:

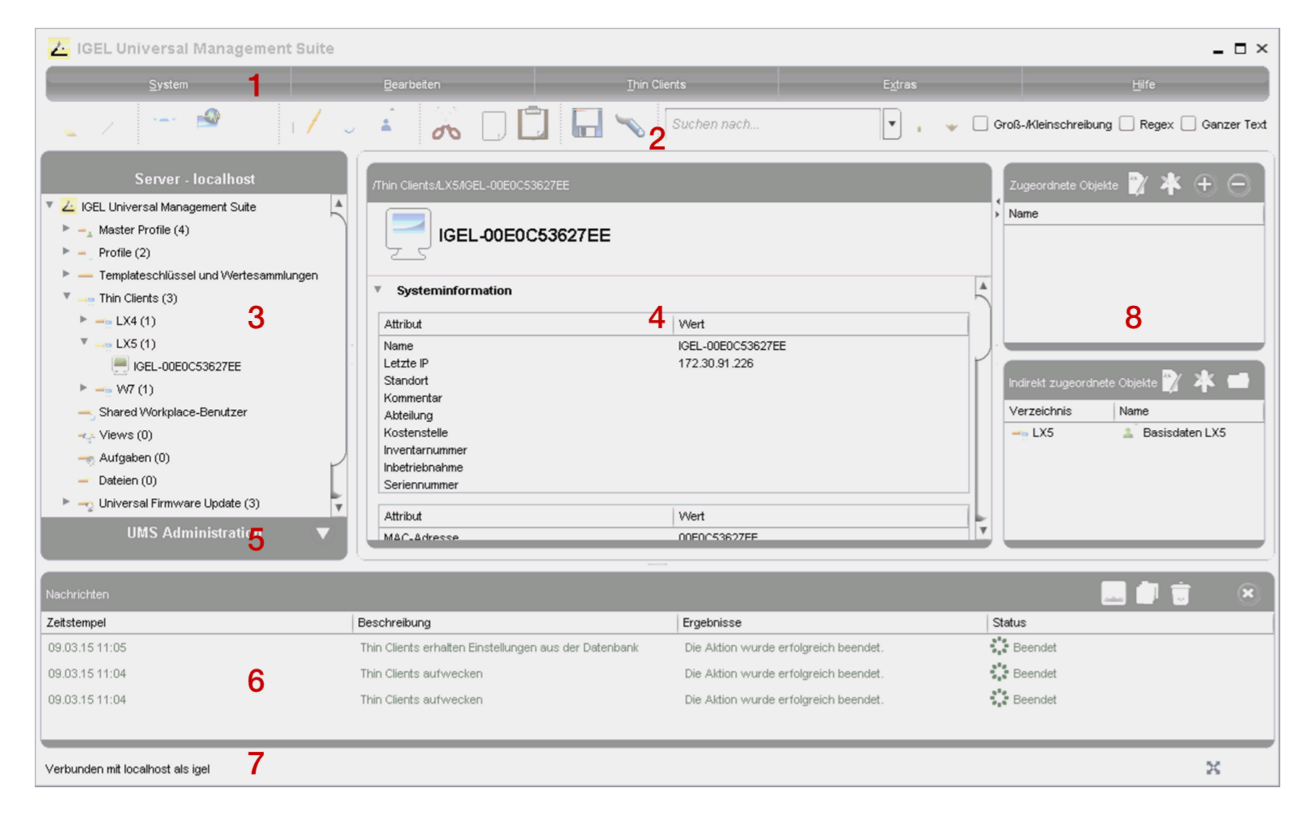


Abbildung 8: Das UMS-Konsolenfenster

1	*Menüzeile* (Seite 29)	Alle Befehle und Aktionen können aus dem Menü heraus gestartet werden. Sie können Shortcuts (Alt + unterstrichenes Zeichen des Menüelements) verwenden, um über die Tastatur auf die Menüleiste zuzugreifen.
2	*Symbolleiste* (Seite 32)	Häufig verwendete Befehle, die Objekte im Navigationsbaum betreffen.
3	*Navigationsbaum* (Seite 32)	Zugriff auf alle UMS-Objekte wie am UMS-Server registrierte Thin Clients, Verzeichnisse, Profile, Ansichten (Views) und geplante Aufgaben.
4	*Inhaltsbereich* (Seite 35)	Informationen zum ausgewählten Objekt (Die meisten Eingabefelder können direkt bearbeitet werden.)
5	*UMS-Administration* (Seite 35)	Verwalten von Aufgaben wie z.B. die Konfiguration der Domänen, des Universal Firmware-Updates und das zeitgesteuerte Backup der UMS-Datenbank (nur Embedded-DB)
6	*Nachrichten* (Seite 35)	Anzeige von Aktionen, die in der UMS-Konsole gestartet werden. Grüner Text weist auf erfolgreiche Vorgänge hin. Rote Zeilen heben ein Problem während der Ausführung des Befehls hervor.
7	*Statuszeile* (Seite 36)	Statusmeldungen der Konsole wie z.B. der aktuell verbundene Server und der Benutzername.
8	*Kontextmenü* (Seite 37)	Objekte wie Profile und Dateien, die den Thin Clients oder Ordnern (direkt oder indirekt) zugeordnet sind.

4.1.1. Menüzeile

Am oberen Rand des Konsolenfensters finden Sie die kontextabhängige **Menüzeile**.

Sie besteht aus den fünf Menüs **System**, **Bearbeiten**, **Thin Clients**, **Extras** und **Hilfe**.

System

Menü → System

Verbinden / Trennen	Erstellen und Trennen der UMS-Server-Verbindung
Erneuern	Aktualisieren der Ansicht
Neu	Anlegen neuer UMS-Objekte wie Verzeichnis, Profil, Aufgabe etc.
Importieren/Exportieren	Importieren und exportieren von Objekten wie Firmware, Profil, Thin Client
Administratorkonten	Anlegen und Verwalten von UMS-Benutzerkonten und -gruppen
Snapshots verwalten	Verwalten von Strukturen auf dem Webserver der UMS
Logging	Anzeige der Nachrichten- und Ereignis-Logs sowie Export der Logs
Lizenzen verwalten	Erstellung und Zuweisung von Firmware-Lizenzen an Thin Clients
VNC-Viewer	Spiegeln eines Thin Client
Customization Builder öffnen *	Starten des Universal Customization Builders, siehe dazu im *Anhang UCB* (Seite 152).
Beenden	Beenden der UMS-Konsolenanwendung

* falls lizenziert

Bearbeiten

Menü → Bearbeiten

Beschreibungsdaten speichern	Speichern geänderter Daten des Inhaltsbereichs
Konfiguration bearbeiten	Konfigurationsparameter von Thin Client oder Profil
Objekte hierher verschieben	Verschiebung ausgewählter Objekte
Umbenennen, Löschen	Objektaktionen im Baum
Berechtigungen	Verwalten der Rechte am ausgewählten Objekt für Benutzer und Gruppen
Ausschneiden, Kopieren, Einfügen	Objektaktionen im Baum

Thin Clients

Menü → Thin Clients

Thin Client Befehle (Standbymodus, Herunterfahren...)	Befehle, die an Thin Clients abgesetzt werden können. Z. B. Herunterfahren, neu starten, Firmware Update, Einstellungen senden/empfangen, Nachricht senden, etc.
Einstellungen übernehmen von...	Senden von Profileinstellungen einmalig an den Thin Client
Änderungsstatus der Konfiguration zurücksetzen	Zurücksetzen der Änderungsmarkierungen (blauer Punkt an den Icons der Thin Clients)
Templatewerte-Zuordnungen überprüfen *	Überprüfen der Zuordnung von Templatewerten
Thin Clients scannen	Suchen nach Thin Clients im Netzwerk des UMS-Servers

* falls Feature aktiviert

Extras

Menü → Extras

Vorgabeverzeichnisse	Automatische Verzeichniszuordnung von Thin Clients nach Regeln
Suchen	Suche nach Objekten
Geplante Aufgaben	Verwaltung von Feiertagslisten und Zuweisung von Aufgaben an Hosts
Passwort ändern	Änderung des Passworts des angemeldeten Benutzers
SQL-Konsole	Direkter Zugriff auf die Datenbank mit SQL-Skripten
Firmware-Statistik	Auflistung der in der Datenbank registrierten Firmware-Versionen
Unbenutzte Firmware entfernen	Löschen von Firmware-Versionen aus der Datenbank, die von keinem Thin Client und keinem Profil verwendet werden
Cache verwalten	Einsehen, aktualisieren und leeren des UMS-Server-Cache
Einstellungen	Konfigurationsparameter wie Sprache der Konsole, Time-out-Werte der Onlineprüfung oder Universal Firmware-Updatesuche etc.

Warnung: Die SQL-Konsole ist ausschließlich für administrative Zwecke vorgesehen. Sie können mit Operationen auf der Konsole die Datenbank zerstören.

Hilfe

Menü → Hilfe

Hilfe	Link zum Handbuch auf edocs.igel.com
IGEL Knowledge Base	Link zu weiterer Online-Dokumentation auf edocs.igel.com
Supportinformation speichern...	Speichern von Logdateien von UMS Server und Konsole in einer `ZIP`-Datei
TC-Dateien für den Support speichern	Speichern von Log- und Konfigurationsdateien eines Thin Clients in einer `ZIP`-Datei.
Lizenzen von Drittanbietern	Auflistung der Lizenzen von in der UMS verwendeter Fremdsoftware und Bibliotheken wie z. B. von Apache Tomcat
Info	Anzeigen der aktuellen Version von UMS-Konsole und Java-Umgebung sowie des angemeldeten Benutzers

4.1.2. Symbolleiste

In der **Symbolleiste** finden Sie Schaltflächen für häufig verwendete Befehle:



Abbildung 9: Die Symbolleiste

In der Reihenfolge der Symbole sind dies:

Aktualisieren	Aktualisiert die Ansicht und den Status der Thin Clients.
Onlineprüfung	Führt eine Onlineprüfung der Thin Clients durch.
Thin Clients scannen	Sucht nach Thin Clients im Netzwerk.
Umbenennen	Ändert Objektnamen im Navigationsbaum.
Löschen	Löscht Objekte im Navigationsbaum.
Berechtigungen	Legt Zugriffsrechte für ausgewählte Objekte fest.
Ausschneiden, Kopieren, Einfügen	Sie können Objekte auch per Drag-and-Drop im Baum verschieben.
Beschreibungsdaten speichern	Speichert bearbeitete Beschreibungsdaten von Thin Clients oder Profilen (Daten im Inhaltsbereich).
Konfiguration bearbeiten	Pflegen Sie Konfigurationsparameter von Thin Clients oder Profilen. Diese entsprechen zumeist den Parametern im lokalen Setup der Clients.
Schritt zurück / vor	Geht in der Konsolenhistorie zurück und vor. Dies betrifft nur die Ansicht (Fokus), keine Aktionen (kein Undo).
Quick Search	Findet Objekte im Navigationsbaum anhand von Name, MAC, IP, ID. Reguläre Ausdrücke (**Regex**) lassen sich verwenden, die letzten 20 Suchanfragen des Benutzers werden gespeichert.

> Der **Schritt zurück/vor** erlaubt lediglich einen Rückblick auf die zuletzt besuchten Objekte. Vorgenommene Änderungen werden nicht rückgängig gemacht!

4.1.3. Navigationsbaum (Management Tree)

Der **Navigationsbaum (Management Tree)** gliedert sich in die Unterbereiche:

Masterprofile	Erstellen und Organisieren der Masterprofile
Profile	Erstellen und Organisieren der Standardprofile
Templateschlüssel und Wertesammlungen	Schlüssel und Werte zur Verwendung in Templateprofilen
Thin Clients	Organisieren der verwalteten Thin Clients in diesem Bereich
Shared Workplace Benutzer	Weist AD-Benutzern spezifische Profile zu
Views	Erstellen von konfigurierbaren Listenansichten von Thin Clients
Aufgaben	Definieren von zeitgesteuerten Aufgaben wie z. B. Firmware-Updates
Dateien	Registrierung von Dateien für die Übertragung an Thin Clients
Universal Firmware Updates	Herunterladen der aktuellen Firmware Versionen zur Verteilung an Thin Clients
Suchhistorie	Gespeicherte Suchanfragen
Papierkorb	Enthält gelöschte und wieder herstellbare Objekte

Über Slider oder Schieberegler können Sie die einzelnen Bereiche in der Größe verändern und ausblenden. Objekte im Navigationsbaum können Sie durch Anklicken markieren bzw. auswählen, eine Mehrfachauswahl ist mit Umschalttaste bzw. Strg möglich.

Unter **Thin Clients** finden Sie alle in der Datenbank registrierten Thin Clients.

> Tipp: Hinter jedem Ordner ist die Anzahl der enthaltenen Elemente angegeben (inkl. der Elemente in Unterordnern). Sie können diese Anzeige im Menü ändern unter **Extras > Einstellungen > Anzahl der Verzeichnisinhalte anzeigen**.

- Wählen Sie ein Verzeichnis aus.

  Im Inhaltsbereich wird die TC-Verzeichnisinhaltsseite angezeigt - mit Informationen zum Inhalt des Verzeichnisses und zugewiesenen Objekten (z. B. Profile).

Jeder Thin Client, der durch seine MAC-Adresse identifiziert ist, kann nur einmal im UMS-Baum angezeigt werden. Sie können einen Thin Client per Drag-and-Drop von einem Verzeichnis in ein anderes verschieben. Der im Baum angezeigte Name wird nur zur Identifizierung des Thin Clients in der UMS verwendet und muss nicht mit dem Namen des Thin Clients im Netzwerk identisch sein – obwohl dieser interne Name auf den Netzwerknamen gesetzt wird, wenn Sie den Thin Client erstmals registrieren. Der TC-Name muss nicht eindeutig sein und kann mehrfach verwendet werden. Das eindeutige Identifizierungsmerkmal ist die MAC-Adresse.

Die Farbe der Thin Clients im UMS-Baum weist auf den jeweiligen Status hin:

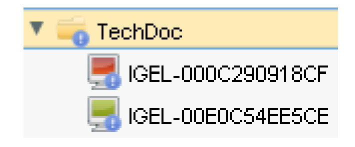


Abbildung 10: Farben im UMS-Baum

- Grün, wenn der Thin Client online ist
- Rot, wenn der Thin Client offline ist
- Ausrufezeichen, wenn Änderungen noch nicht übertragen wurden

Die Erkennung erfolgt automatisch durch regelmäßiges Senden von UDP-Paketen an die Thin Clients, die derzeit in der UMS-Konsole angezeigt werden (Default: alle 3 Sekunden). Sie können diesen Status manuell in der Symbolleiste aktualisieren und das Abfrageintervall für die Online-Prüfung im Menü **Extras→Einstellungen→Online Prüfung** festlegen.

Die Onlineprüfung lässt sich in der Anwendung *UMS Administrator* (Seite 39) komplett deaktivieren.

In der Unterstruktur **Profile** können Sie Profile für Thin Clients oder Thin Client-Verzeichnisse verwalten. Sie haben die Möglichkeit, Verzeichnisse zum Speichern von Profilen zu erstellen und können die Profile in diesem Teil der Struktur hinzufügen, löschen und ändern. Die Informationen zu einem ausgewählten Profil werden im Inhaltsbereich angezeigt. Um ein Profil einem Thin Client zuzuordnen, können Sie den Thin Client entweder per Drag-and-Drop in das Profil ziehen oder umgekehrt. Dies funktioniert auch bei Profilen und Thin Client-Verzeichnissen. Auch über die Schaltfläche **Hinzufügen** der Objektbereiche (8) lassen sich Profile den Thin Clients oder Thin Client-Verzeichnissen zuweisen.

Unter **Views** werden alle erstellten Ansichten der Thin Clients angezeigt. Sie können neue Views erstellen, Views bearbeiten oder löschen und das Ergebnis der View in unterschiedlichen Formaten (z.B. XML) exportieren. Diese Baumstruktur kann auch Unterverzeichnisse für die Anordnung von Views beinhalten.

Wenn Sie die Funktion **IGEL Shared Workplace** verwenden, um beim Login benutzerspezifische Profile an Thin Clients zu verteilen, so ordnen Sie im Bereich **Shared Workplace Benutzer** einem AD-Benutzer oder einer Gruppe ein oder mehrere Profile zu. Auch eine simulierte Ansicht der wirksam werdenden Einstellungen können Sie hier generieren.

Unter **Aufgaben** werden alle festgelegten Aufgaben angezeigt. Sie können neue geplante Aufgaben anlegen und aufgelistete Aufgaben bearbeiten oder löschen. Die Zuweisung von Aufgaben an Thin Clients nehmen Sie in der Detailansicht einer Aufgabe vor. Diese Baumstruktur kann auch Unterverzeichnisse beinhalten, um die Aufgaben zu organisieren.

4.1.4. Inhaltsbereich

Der **Inhaltsbereich**, oder Content Panel, zeigt die Eigenschaften des jeweils im Baum markierten Objekts an. Dies kann der Inhalt eines Verzeichnisses sein, also z. B. die dort abgelegten Profile, Thin Clients, Unterordner, Aufgaben etc., oder Detailinformationen eines Objekts, wie Systeminformationen des Thin Clients, Basisdaten eines Profils, Trefferliste einer View etc.

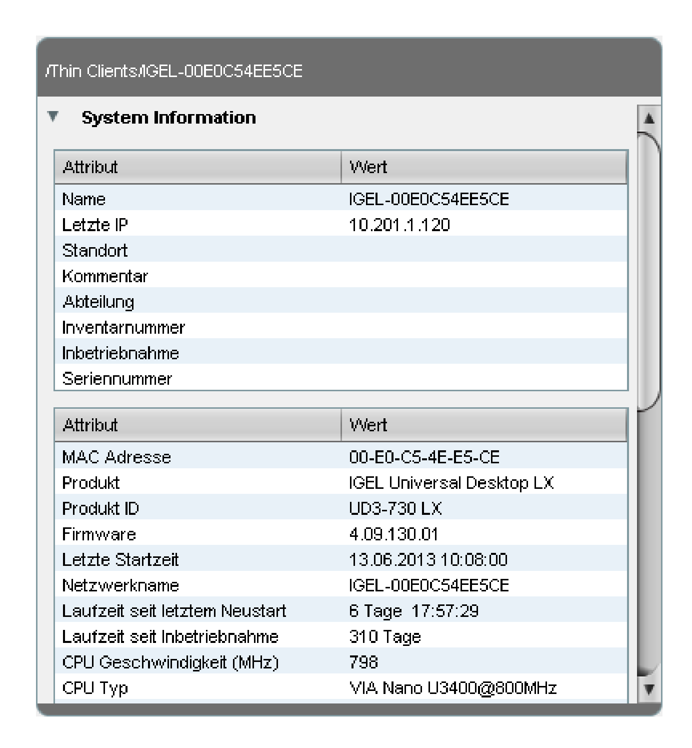


Abbildung 11: Systeminformationen des Thin Clients

4.1.5. UMS Administration

Mit Version 3.09 der IGEL Universal Management Suite wurden einige Einstellungsoptionen vom UMS-Administrator in den Administrationsbereich der UMS-Konsole verlagert. Dort gibt es einen neuen Bereich **UMS Administration**.

Die Konfiguration des Active Directory und der Servereinstellungen des Universal Firmware Updates wurden vom UMS-Administrator in den Administrationsbereich der UMS-Konsole verlagert. Im UMS-Administrator wird auf den zuvor verwendeten Registerkarten ein entsprechender Hinweis angezeigt. Zusätzlich finden Sie hier neue Funktionen wie die alternative Konfiguration von LDAP oder zeitgesteuerte Backups.

4.1.6. Nachrichten

Der Fensterbereich **Nachrichten** enthält Informationen über die erfolgreiche oder fehlerhafte Ausführung von Befehlen. Wenn ein Kommando nicht erfolgreich ausgeführt werden konnte, wird eine rote Nachricht in der Liste angezeigt. Außerdem blinkt ein Warnzeichen in der Statuszeile der UMS-Konsole, bis der Benutzer die Nachricht auswählt.

- Klicken Sie **Ergebnis zeigen** oder doppelklicken Sie die Nachricht, um Details zur Nachricht anzusehen.

- Löschen Sie erledigte Nachrichten oder warten Sie, bis das Nachrichtenfenster bei Beenden der UMS-Konsole automatisch zurückgesetzt wird.
- Ändern Sie die Größe des Nachrichtenfensters über den mittleren Slider oder blenden Sie es ganz aus.

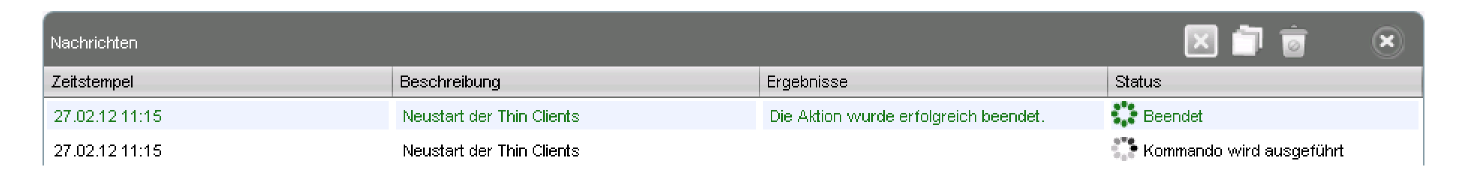


Abbildung 12: Das Nachrichtenfenster

4.1.7. Statuszeile

Die **Statuszeile** zeigt den Namen des aktuell verbundenen UMS-Servers und des an der Konsole angemeldeten Benutzers an. Das Symbol unten rechts signalisiert den Status des Nachrichtenfensters. Z. B. zeigt es an, wenn neue Warnmeldungen vorhanden sind. An dieser Stelle sind sie auch bei ausgeblendetem Nachrichtenbereich zu sehen.

4.1.8. Zugeordnete Objekte

Der Bereich **Zugeordnete Objekte** gliedert sich in zwei Teile, um direkt von indirekt zugewiesenen Objekten schnell unterscheiden zu können.

Direkt zugeordnete Objekte wurden einem einzelnen Thin Client, Ordner oder Profil zugewiesen.

Indirekte Objekte wurden über die Ordnerstruktur 'geerbt'.

- Doppelklicken Sie auf ein Objekt im Zuweisungsbereich um das einem Thin Client zugewiesene Profil direkt zu bearbeiten.

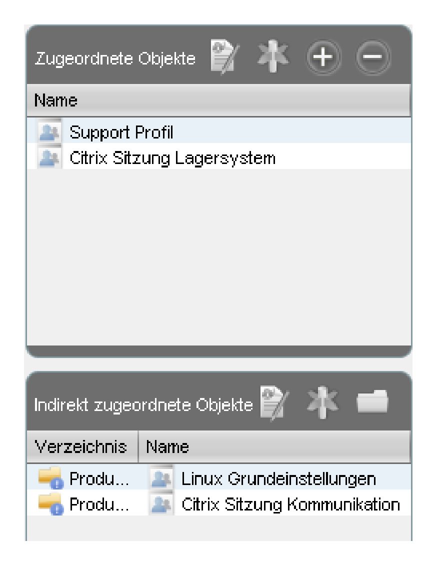
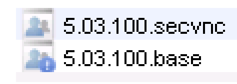


Abbildung 13: Direkt und indirekt zugeordnete Objekte

Zugewiesene Profile mit noch nicht an den Thin Client übertragenen Konfigurationsänderungen werden in der Liste zugeordneter Objekte mit einem Ausrufezeichen markiert:



4.1.9. Kontextmenü

Ein objektabhängiges **Kontextmenü** erhalten Sie durch Rechtsklick auf das entsprechende Objekt. Je nach Auswahl stehen Aktionen für Ordner, Thin Clients, Shared Workplace Benutzer usw. zur Verfügung. Das gewählte Kommando wird für alle zuvor im Baum markierten Objekte ausgeführt.

Manche Kommandos lassen sich nur für einzelne Objekte, nicht aber für Verzeichnisse mit Objekten ausführen. Diese Optionen sind im Menü dann deaktiviert. Beispiel: Das Kommando **Datei TC > UMS** kann nur für einen einzelnen Thin Client ausgeführt werden, das Kommando **Datei UMS > TC** hingegen für alle Thin Clients in einem Verzeichnis.

4.1.10. Suche nach Objekten in der UMS

Objekte innerhalb des UMS-Navigationsbaums lassen sich über folgende Wege finden:

- Quick Search
- Suchfunktion
- View

Die **Quick Search** in der Symbolleiste bietet den schnellsten Zugriff auf die Suchfunktion. Die Eingabemaske ist im Konsolenfenster immer sichtbar. Die Tastenkombination Umschalt-Strg-F setzt den Cursor direkt in das Eingabefeld. Die Suchanfragen der **Quick Search** sind begrenzt auf wenige Objekteigenschaften: Objektname, Objekt-ID, MAC-Adresse, IP-Adresse. Diese Daten werden zum Start der Konsole lokal gepuffert und sind somit ohne Datenbankzugriff sehr schnell durchsuchbar. Die letzten 20 Suchanfragen des Benutzers werden für den schnellen Zugriff gespeichert - allerdings nicht in der UMS-Datenbank, sondern in den Systembenutzerdaten des Konsolenbenutzers (Windows Registry).

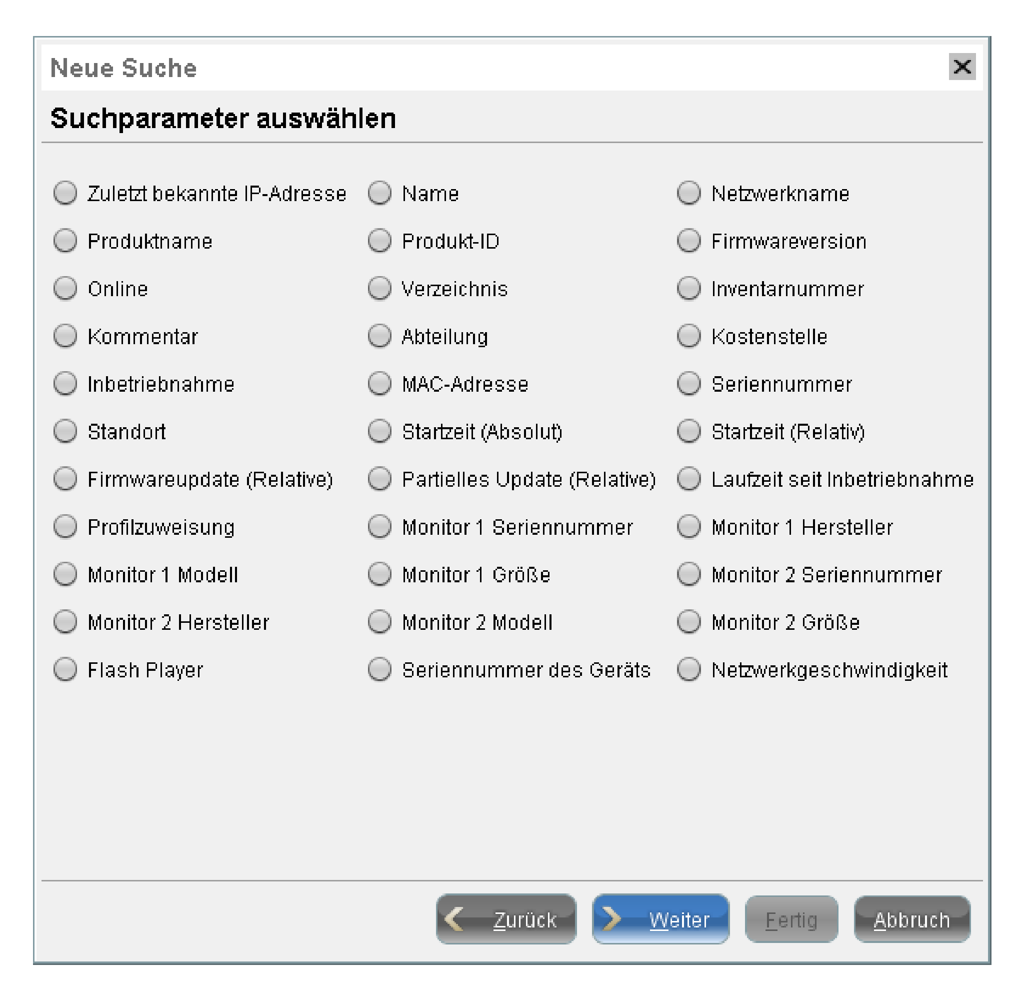


Abbildung 14: Suchparameter für Thinclients

Die normale Suchfunktion der UMS (Menü **Extras→Suchen** oder Tastenkombination Strg-F) stellt umfangreiche Optionen zur Suche auf der UMS-Datenbank bereit. Neben den Daten der schnellen Suche (s.o.) stehen hier auch alle anderen Daten von Thin Clients, Profilen oder Views zur Auswahl - z.B. die selbst vergebene Inventarnummer oder das Modell des angeschlossenen Monitors. Verschiedene Kriterien lassen sich logisch verknüpfen (UND / ODER). Die Suchanfragen des Benutzers werden im Navigationsbaum unter **Suchhistorie** abgelegt und lassen sich so einfach bearbeiten und erneut verwenden.

Sehr ähnlich wie Suchanfragen funktionieren **Views** (Seite 96), auch hier lassen sich verschiedene Kriterien verknüpfen und die Anfrage speichern. Anders als Suchanfragen stehen **Views** jedoch allen UMS-Administratoren - abhängig von ihren Berechtigungen - gemeinsam zur Verfügung. Außerdem lassen sich **Views** auch in die Definition *geplanter Aufgaben* (Seite 103) einbinden.

4.1.11. Löschen von Objekten in der UMS / Papierkorb

Mit der IGEL Universal Management Suite ab Version 4.07.100 haben Sie nun auch die Möglichkeit, Objekte im **Papierkorb** abzulegen, anstatt sie sofort dauerhaft zu löschen. Der Papierkorb wird global für alle Benutzer der UMS aktiviert oder deaktiviert.

- Aktivieren Sie den Papierkorb im Administrationsbereich unter **Zusätzliche Einstellungen→Papierkorb aktivieren**.

Wird nun ein Objekt im Navigationsbaum gelöscht (Funktion **Löschen** in der Symbolleiste, im Kontextmenü oder Taste Entf), so wird es nach Bestätigung in den Papierkorb verschoben.

> Bei aktivem Papierkorb lassen sich Objekte auch direkt und entgültig löschen mit Umschalt-Entf.

Verzeichnisse werden mitsamt ihrer Unterordner und aller Elemente in den Papierkorb verschoben und können so als komplette Struktur auch wiederhergestellt werden. Den UMS-Papierkorb finden Sie als untersten Knoten im Navigationsbaum der UMS-Konsole. Elemente im Papierkorb lassen sich dort entgültig löschen oder auch wiederherstellen - rufen Sie dazu das Kontextmenü eines Elements im Papierkorb auf.

> Sollte sich das Kontextmenü für Elemente im Papierkorb nicht aufrufen lassen, so ist der Papierkorb wahrscheinlich inaktiv. Prüfen Sie den Status des Papierkorbs wie oben beschrieben.

Es lassen sich fast alle Elemente aus dem UMS-Navigationsbaum in den Papierkorb verschieben: Thin Clients, Profile, Views, Aufgaben, Dateien und deren Verzeichnisse. Nicht löschen lassen sich Shared Workplace-Benutzer, nur endgültig löschen lassen sich Administratorkonten (in der Kontenverwaltung) und Elemente der Suchhistorie (mit Umschalt-Entf). Ebenfalls nicht gelöscht werden können die jeweils obersten Knoten im Navigationsbaum - allerdings wirkt sich dieser Vorgang auf alle löschbaren Elemente unterhalb dieses Knotens aus!

- Objekte im Papierkorb werden weder von der Suchfunktion noch durch Views gefunden und lassen sich auch nicht durch geplante Aufgaben ansprechen.
- Thin Clients im Papierkorb erhalten keine neuen Einstellungen von der UMS mehr, bleiben aber an der UMS registriert und können aus dem Papierkorb mit allen Profilzuordnungen wiederhergestellt werden.
- Profile im Papierkorb sind nicht mehr wirksam, es ändern sich ggf. also Einstellungen von Thin Clients. Die Wiederherstellung von Profilen lässt auch deren Zuordnungen zu Thin Clients wieder aktiv werden.
- Geplante Aufgaben, Views und Suchanfragen im Papierkorb werden nicht ausgeführt.
- Zuordnungen von Profilen, Dateien, Views und Firmware Updates im Papierkorb sind nicht aktiv.

4.2. Der IGEL UMS–Administrator

Die IGEL UMS-Administratoranwendung ist nur auf einem UMS-Server verfügbar, weil damit direkt in die Kommunikation der Dienste eingegriffen werden kann. Mit ihr lassen sich z. B. Basisdaten wie verwendete Ports oder angebundene Datenquellen bearbeiten. Diese Funktionen stehen in der Konsole im Administrationsbereich nicht zur Verfügung.

Die Serverkonfiguration des Administrators lässt sich für Backups über **Datei** exportieren und wieder importieren. Unter **Datei→Einstellungen→Sprache** können Sie die Sprache des Administratortools ändern.

> Die Berechtigungen für die Änderung von Einstellungen sind davon abhängig, ob eine Berechtigung für die Änderung der IGEL UMS-Dateien auf dem Serversystem besteht. Sie sollten daher für die Verwendung des IGEL UMS-Administrators dasselbe Benutzerkonto verwenden, mit dem Sie die Installation der UMS durchgeführt haben.

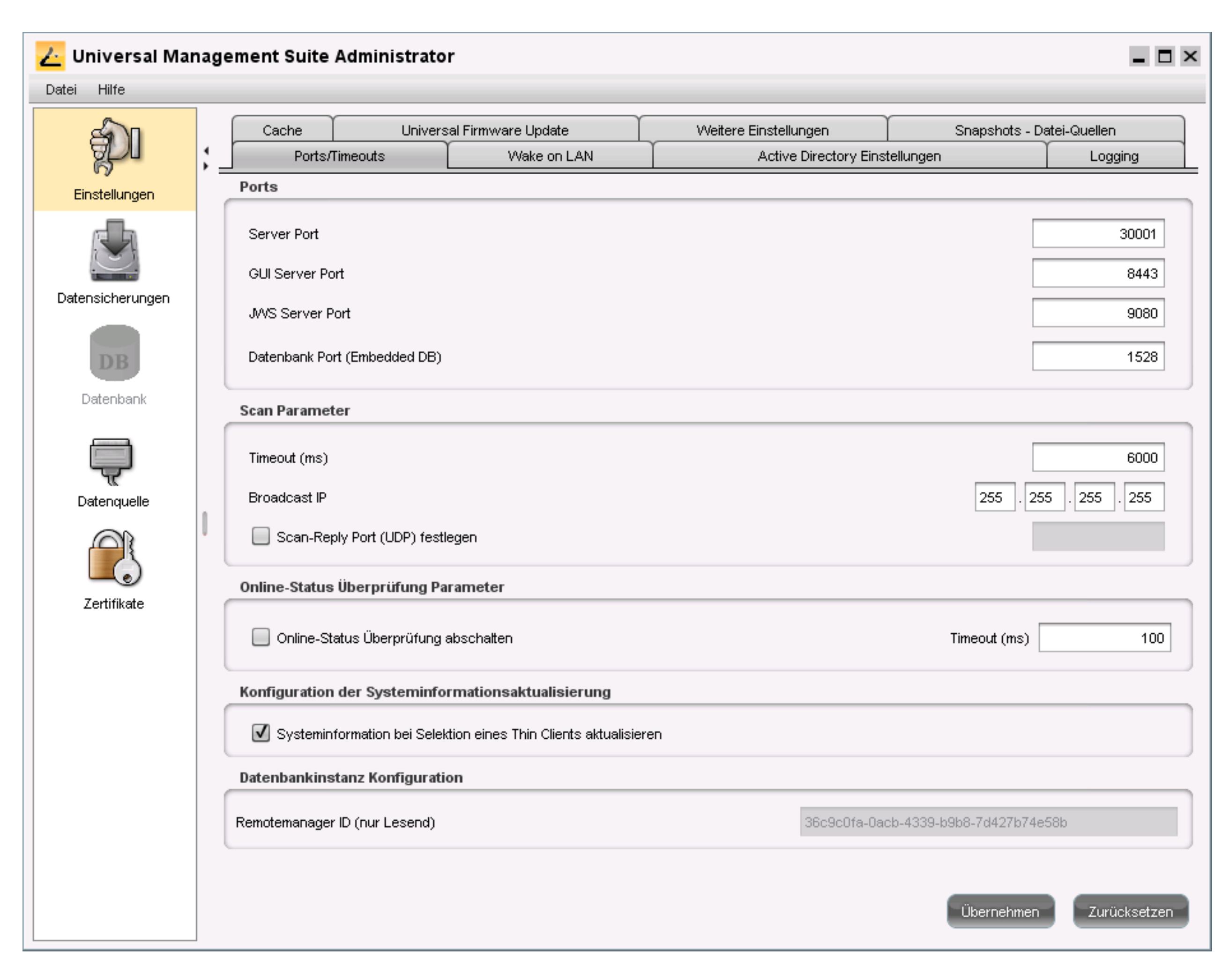


Abbildung 15: Der UMS-Administrator

4.2.1. Servereinstellungen

Über den UMS-Administrator können Sie verschiedene Einstellungen am Server vornehmen.

Ports/Zeitlimits

Beim Start der Anwendung wird der Fensterbereich **Einstellungen** des UMS-Administrators angezeigt. Hier können Sie von der UMS verwendete Ports und andere zugehörige Einstellungen wie das Zeitlimit usw. eingeben.

Der IGEL UMS-Server verwendet diese offenen Ports für eingehende Anfragen:

Portname	verwendet durch	Aufgabe
Serverport	TC-Server	Die Thin Clients verbinden sich mit diesem Port. Der Standardport ist `30001`. Änderungen an diesem Port dürfen nur durchgeführt werden, wenn gleichzeitig sicher gestellt wird, dass Thin Clients die Verbindungsaufnahme ebenfalls auf dem neuen Port durchführen!
GUI Serverport (HTTPS)	IGEL UMS-Konsole	Stellt die Verbindung zum Server her. Sie müssen diesen Port im Anmeldefenster der IGEL UMS-Konsole eingeben, das ist standardmäßig `8443`.
JWS Serverport (HTTP)	Java Web Start-Schnittstelle	Dieser Port ermöglicht ein Starten der UMS Konsole per Java Web Start über eine nicht verschlüsselte Verbindung. Dazu müssen Sie diesen Port in der Verbindungs-URL angeben, z. B. `http://hostname:9080/start_rm.html`. Der Standardwert ist `9080`.
DB-Port		Die Kommunikation mit der **Embedded-DB** erfolgt auf Port `1528`, für externe Datenbanken pflegen Sie den Port unter **Datenquellen**.

➢ Aktivieren Sie die Option **Verbindung nur über SSL zulassen**, um den Netzwerkverkehr der IGEL UMS zu verschlüsseln. Java Web Start ist dann nur noch über den GUI Serverport (Standardwert 8443) möglich.

> Verwenden Sie die Option **Verbindung nur über SSL zulassen** nicht, wenn Sie Windows Embedded 7 in einer Version 3.08.100 oder älter einsetzen und zudem das Feature Universal Firmware Update nutzen möchten. Diese älteren Windows-Firmwares unterstützen Firmwareupdates über HTTPS nicht.

Im Bereich **Scanparameter** können folgende Werte konfiguriert werden:

Zeitlimit (ms) Hier wird festgelegt, wie lange die IGEL UMS auf eine Antwort auf Scanpakete warten soll, die an das Netzwerk gesendet wurden. Dieser Wert ist in Millisekunden angegeben und standardmäßig auf 6000 gesetzt.

Broadcast-IP Broadcast-Adresse, die für Scanpakete verwendet wird. Sie wird nur zum Scannen des lokalen Netzwerks verwendet. Wenn IP-Bereiche genutzt werden, werden die UDP-Pakete an jeden Client im IP-Bereich versendet. Die Standardeinstellung ist hier 255.255.255.255. Diese muss normalerweise nicht geändert werden.

Scan-Reply Port (UDP) festlegen Einstellung eines festen Ports, auf dem die Thin Clients antworten, wenn Sie mit UDP scannen. Bei der Verwendung von TCP wird dieser Port nicht benötigt, da die Antwort auf einem eingerichteten Socket erfolgt. Wenn Sie die Standardeinstellung lassen und keinen Port festlegen, wählt die Anwendung einen beliebigen freien Port aus.

Im Bereich **Parameter für Onlineüberprüfung** gibt **Zeitlimit** an, wie lange auf die Antwort einer Onlinestatus-Abfragenachricht gewartet wird. Die IGEL UMS-Konsole versucht, alle Thin Clients zu kontaktieren, die in der Konsole gerade sichtbar sind. Jeder Thin Client in diesem Bereich muss in der vorgegebenen Zeit auf die Statusanfrage antworten oder wird als offline markiert. Der Standardwert ist 100 ms.

So deaktivieren Sie die Onlinestatus-Prüfung:

➢ Wählen Sie **Überprüfung des Onlinestatus abschalten**.

Sie können die Onlineprüfung auch auf der UMS-Konsole deaktivieren. Der Unterschied ist, dass in diesem Fall die Funktion nur für diese eine Konsoleninstallation deaktiviert ist.

Weitere Einstellungen

Hier lassen sich einige weitere allgemeine Parameter konfigurieren:

Anfragen der Thin Clients	Sie können die Zahl der akzeptierten gleichzeitigen Anfragen, wie `get_settings_on_boot`, begrenzen, falls es z. B. bei einer großen Zahl zeitgleich bootender Clients zu Problemen kommt. Besser setzen Sie jedoch in diesem Fall ein UMS-High-Availability-Netzwerk ein, um die Clientanfragen auf mehrere UMS-Server zu verteilen.
Geplante Aufgaben	Definieren Sie die Ablaufzeit für geplante Aufgaben.
Anpassen von Thin Client Namen	In der UMS-Konsole können Sie Thin Clients einen Gerätenamen geben. Die Thin Clients haben im Netzwerk einen Namen – standardmäßig ist das `IGEL-<MAC Adresse>`. Sie können nun beides synchron halten: • Wählen Sie **UMS-internen Namen anpassen**, um in der UMS den Netzwerknamen des TC zu verwenden. • Wählen Sie **Netzwerknamen anpassen**, um den in der UMS gepflegten Namen auch als Gerätenamen zu verwenden.
Automatisch Registrieren	Aktivieren Sie die automatische Registrierung von IGEL-Thin Clients, die im Netzwerk booten.

Snapshot-Dateiquellen

Erstellen Sie **Webressourcen** im Ordner **WebDAV**, die Sie mit dem UMS-internen Webserver Tomcat verwenden.

Über diese Ressourcen können Sie den Thin Clients Dateien zur Verfügung stellen, wie z. B.

- Firmware Updates
- Partielle Updates
- Hintergrundbilder
- Virenscanner-Signaturen usw.

So erstellen Sie eine neue Webressource:

1. Klicken Sie **Neu**.
2. Definieren Sie einen Namen für die Ressource unter **Öffentlicher Name** .
3. Wählen Sie das **Dokumentbasisverzeichnis**, auf welches die Ressource zeigen soll.
4. Klicken Sie **OK**.

So testen Sie den Zugriff auf die neue Webressource:

1. Starten Sie einen Browser.
2. Geben Sie die Adresse der Webressource ein: http://<UMS-Server>:9080/<öffentlicher Name>
3. Melden Sie sich an der Ressource mit einem UMS-Administratorkonto an.

4.2.2. Datensicherungen

Die interne Embedded-DB des UMS-Servers kann direkt über den UMS-Administrator gesichert werden. Es lassen sich auch zuvor erstellte Backups wieder einspielen. Für externe Datenbanksysteme verwenden Sie bitte die vom DBMS-Hersteller vorgesehene Vorgehensweise zu Backup und Recovery. Zertifikate müssen in diesem Fall separat gesichert werden.

Backup erstellen

So erstellen Sie ein Backup:

1. Klicken Sie **Ändern** neben dem **Verzeichnis** Eingabefeld, um das Zielverzeichnis zu ändern.

   Das Dateiauswahlfenster wird geöffnet.
2. Legen Sie den Speicherort für Ihre Backups fest.
3. Klicken Sie **Erzeugen**.
4. Geben Sie einen Namen für dieses Backup in das Pop-up-Fenster ein.

   Die Daten werden in dem von Ihnen gewählten Verzeichnis gespeichert.
   Die Zertifikatsdateien `server.pem` und `server.crt` werden ebenfalls in das Backup aufgenommen.

Backup wiederherstellen

> Ihr aktueller Datenbankstatus wird überschrieben. Es wird dringend empfohlen, ein Backup der aktuellen Daten zu erstellen, bevor ein anderes Backup wiederhergestellt wird.

So stellen Sie ein gespeichertes Backup wieder her:

1. Wählen Sie das gewünschte Backup aus der Backupliste aus.
2. Klicken Sie auf **Wiederherstellen**.
3. Nach erfolgter Wiederherstellung werden die Anmeldedaten zur Datenbank angezeigt.

Backup löschen

So löschen Sie ein gespeichertes Backup:

1. Wählen Sie das gewünschte Backup aus der Backupliste aus.
2. Klicken Sie **Löschen**, um nicht mehr benötigte Backups zu entfernen.

   > Es wird sowohl der Eintrag im UMS-Administrator wie auch die Backupdatei auf der Festplatte gelöscht!

Backup auf der Kommandozeile

Darüber hinaus steht ein Befehlszeilenprogramm für die Erstellung eines Backups mit Batchdateiskripts zur Verfügung. Es heißt `embackup.exe`, und Sie finden es im Installationsverzeichnis der UMS im Verzeichnis **rmadmin**.

Sie können das Programm mit den folgenden Optionen starten:

`b path/filename:`	der Pfad und der Name der Backupdatei, die erstellt wird
`r path/filename:`	die Backupdatei mit dem angegebenen Pfad wird in der Datenbank wiederhergestellt
`u username:`	UMS-Benutzername
`p password:`	Passwort des UMS-Benutzers

Zeitgesteuertes Backup

Siehe *Geplantes Backup (Embedded-DB)* (Seite 119)

4.2.3. Datenquellen

Die Anbindung an ein Datenbanksystem erfolgt über Datenquellen, die Sie im UMS-Administrator verwalten. Haben Sie die Standardinstallation gewählt, ist die Embedded-DB bereits als Datenquelle eingerichtet und aktiviert.

Siehe auch: *Anbindung externer Datenbanksysteme* (Seite 17)

Datenquelle anlegen

1. Klicken Sie auf **Neu**, um eine erste oder weitere Datenquelle hinzuzufügen.

   Es öffnet sich ein Dialogfenster.

2. Wählen Sie den Typ des DBMS, den Host / Port für den Verbindungsaufbau sowie den am DBMS eingerichteten Benutzer. Für SQL Server Cluster und Oracle RAC ist die Instanz anzugeben.

   Näheres zu den einzelnen unterstützten DBMS finden Sie im UMS-Datenblatt auf der IGEL-Webseite und im *Anhang UMS HA* (Seite 143).

   > Solange eine Datenquelle nicht aktiviert wurde, lassen sich diese Einstellungen über **Ändern** noch anpassen. Die aktive Datenquelle ist vor Konfigurationsänderungen geschützt. Über **Passwort ändern** können Sie ein neues Passwort für den Datenbankbenutzer setzen. Das ist auch bei aktivierter Datenquelle möglich.

3. Klicken Sie **Test**, um die Verbindung zur Datenbank zu testen.

   Das ist auch bei inaktiven Datenquellen möglich.

Datenquelle aktivieren

Sie können mehrere Datenquellen anlegen. Es kann aber nur eine aktiv vom Server verwendet werden.

So aktivieren Sie diese Datenquelle:

1. Wählen Sie aus der Liste der eingerichteten Datenquellen eine aus.
2. Klicken Sie **Aktivieren**.
3. Geben Sie das Passwort für die ausgewählte Datenquelle ein.

   Während der Aktivierung der Datenquelle prüft die Anwendung, ob ein gültiges Datenbankschema gefunden werden kann. Wenn kein Schema gefunden wird, erfolgt die Erstellung eines neuen Schemas. Ein veraltetes Schema wird aktualisiert, und wenn das Schema unbekannte Daten enthält, werden diese überschrieben.
4. Bestätigen Sie jede dieser Aktionen.

Warnung: Das Überschreiben vorhandener Daten bedeutet, dass das gesamte Datenbankschema gelöscht wird, nicht nur die von IGEL UMS verwendeten veralteten Tabellen.

Datenquelle kopieren

So steigen Sie von der Standardinstallation mit Embedded-DB auf ein externes Datenbanksystem um, z. B. auf ein Oracle RAC-Cluster:

1. Bereiten Sie die neue Datenbank entsprechend der UMS-Installationsanweisung vor.
2. Legen Sie eine passende neue Datenquelle für dieses DBMS an.
3. Wählen Sie die noch aktive Datenquelle der Embedded-DB aus.
4. Klicken Sie **Kopieren**.
5. Wählen Sie die Zieldatenquelle aus.
6. Starten Sie den Prozess nach Eingabe der Anmeldedaten des Ziels.
7. Aktivieren Sie die neue Datenquelle.

Aktive Embedded-DB optimieren

- Klicken Sie **Datenbank optimieren**, um eine aktive Embedded-Datenbank zu optimieren.

  Der Datenbankinhalt wird neu strukturiert.
  Der Datenbankindex wird neu erstellt, um die Operationen auf der Datenbank zu beschleunigen.
  Ein Nachrichtenfenster informiert über den erfolgreichen Abschluss dieses Vorgangs.

4.2.4. Zertifikate

Über den Fensterbereich **Zertifikate** können Sie Serverzertifikate speichern, wiederherstellen und konvertieren, so z. B. vom Remote Manager 2.x in das jeweils aktuelle Format.

Eine exportierte KeyStore−Datei können Sie auch bei einer Neuinstallation der IGEL UMS importieren.

5. Thin Clients

Zentraler Bestandteil des Navigationsbaums ist der Knoten **Thin Clients**. Hier organisieren und verwalten Sie alle Geräte, die am UMS-Server registriert sind. IGEL-Thin Clients ebenso wie mit UDC2 installierte Fremdgeräte. Wie Sie Thin Clients in die Datenbank aufnehmen, ist beschrieben in *Registrierung von Thin Clients am UMS Server* (Seite 20).

5.1. Thin Clients verwalten

In der IGEL UMS können Sie Thin Clients über einen Navigationsbaum in Verzeichnisse sortieren. Nutzen Sie die Möglichkeit, um z. B. räumlich oder strukturell zusammengehörige Geräte einfach mit gleichen Profilen versorgen zu können oder um die Thin Clients entsprechend Ihrer Unternehmensstruktur zu ordnen.

5.1.1. Verzeichnis erstellen

Sie können beliebig viele Verzeichnisse und Unterverzeichnisse erstellen, um die Thin Clients in Gruppen zusammenzufassen. Wenn Sie Unterverzeichnisse erstellen, bilden die darin organisierten Thin Clients Untergruppen einer Gruppe.

> Ein Thin Client, der durch seine MAC-Adresse eindeutig identifiziert ist, kann nur in einem einzigen Verzeichnis abgelegt sein, also nur Mitglied einer einzigen Gruppe sein.

So erstellen Sie ein Verzeichnis oder Unterverzeichnis:

1. Wählen Sie ein Verzeichnis, z. B. **Thin Clients**.
2. Klicken Sie in der Hauptmenüleiste **System→Neu →Neues Verzeichnis**

   oder wählen Sie aus dem Kontextmenü des ausgewählten Verzeichnisses die Option **Neues Verzeichnis**.
3. Geben Sie den Namen für das neue Verzeichnis ein.
4. Klicken Sie **OK**.

   Das neue Verzeichnis wird im Navigationsbaum direkt unter dem ausgewählten Verzeichnis angezeigt.

Nun können Sie Thin Clients in dieses neue Verzeichnis verschieben.

5.1.2. Verzeichnis importieren

Wenn Sie eine komplexe Verzeichnisstruktur planen, müssen Sie diese nicht schrittweise in der UMS-Konsole erstellen. Sie können stattdessen eine `csv`-Datei erstellen, z. B. mit einem Tabellenkalkulationsprogramm, in der Sie die Verzeichnisstruktur bestimmen, und die Struktur aus dieser Liste importieren.



Abbildung 16: UMS-Strukturbaum

Der oben abgebildeten Baumstruktur liegt folgende Datei zugrunde:

```
Thin Clients; Augsburg; TD
Thin Clients; Augsburg; QS
Thin Clients; Augsburg; Development
Thin Clients; Bremen; Support
Thin Clients; Bremen; PreSales
```

So importieren Sie eine Verzeichnisstruktur aus einer `csv`-Datei:

1. Wählen Sie aus dem Hauptmenü **System→Importieren→Verzeichnisse importieren**.

   Das Fenster **Verzeichnisse importieren** öffnet sich.

2. Klicken Sie auf **Datei Öffnen**, um eine `csv`-Datei zu laden.

   > In der ersten Spalte müssen Sie eines der vorgegebenen Stammverzeichnisse festlegen, so können Sie auch Verzeichnisstrukturen für Profile, Aufgaben, Views oder Dateien importieren.

3. Klicken Sie auf **Verzeichnisse importieren**, um die Verzeichnisstruktur zu erstellen.

Es öffnet sich ein Fenster mit dem Importergebnis. Neu erstellte Verzeichnisse sind dabei unterstrichen.

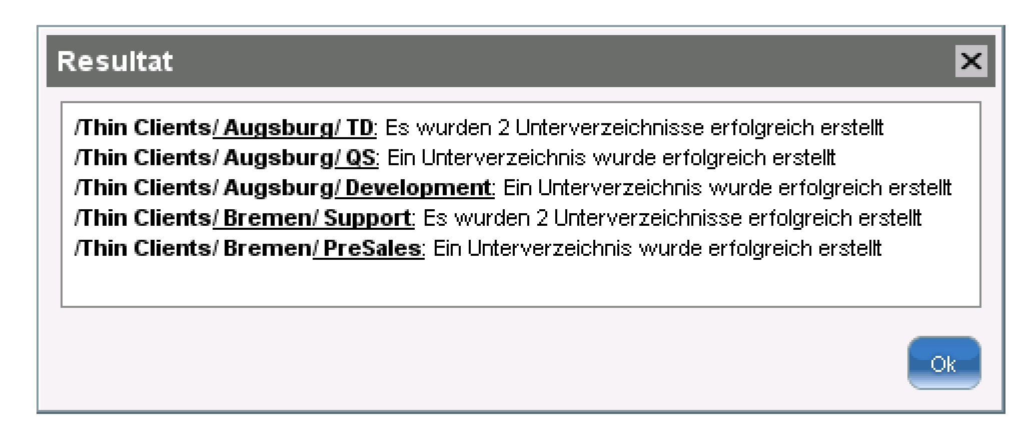


Abbildung 17: Resultat des Verzeichnisimports

5.1.3. Verzeichnis löschen

So löschen Sie ein Verzeichnis:

1. Markieren Sie das zu löschende Verzeichnis.

> Löschen Sie das Verzeichnis im Navigationsbaum und nicht im Inhaltsbereich des Konsolenfensters, da sonst der gesamte Verzeichnispfad mit gelöscht wird.

2. Klicken Sie **Löschen** im Kontextmenü des Verzeichnisses

   oder klicken Sie **Löschen** in der Symbolleiste
   oder klicken Sie die Entf-Taste.
   Eine Liste mit allen zu löschenden Objekten wird angezeigt.

> Wird ein Verzeichnis gelöscht, so werden auch alle darin enthaltenen Unterverzeichnisse und Objekte, wie Thin Clients, Profile oder Views, gelöscht.

3. Bestätigen Sie den Löschvorgang mit **OK**.

5.1.4. Thin Clients verschieben

Drag-and-Drop ist die einfachste Möglichkeit, Thin Clients aus einem Verzeichnis in ein anderes zu verschieben:

1. Halten Sie die Strg-Taste gedrückt, wenn Sie mehrere Clients auswählen möchten.
2. Verwenden Sie die Umschalt-Taste, um eine Reihe von Thin Clients auszuwählen.
3. Bestätigen Sie die Verschiebung mit **Ja**.

   Das Fenster **Änderungszeitpunkt** öffnet sich.

> Werden dem Thin Client durch die Neuzuordnung zu einem Verzeichnis indirekt Profile zugewiesen oder entzogen, so ändert sich seine Konfiguration. Diese wird entweder sofort oder beim nächsten Neustart wirksam.

4. Wählen Sie aus, wann die Änderungen wirksam werden sollen und bestätigen Sie mit **OK**.

Diese beiden Bestätigungsdialoge können Sie im jeweiligen Fenster deaktivieren. Dies lässt sich unter **Extras→Einstellungen→Allgemein** wieder rückgängig machen.

5.1.5. Regeln für Vorgabeverzeichnisse definieren

Definieren Sie Regeln für Vorgabeverzeichnisse. Die Thin Clients werden bei der Registrierung entsprechend dieser Regeln automatisch in bestimmte Verzeichnisse des Baums abgelegt. Sie erhalten die Einstellungen der Profile dieser Verzeichnisse. Sie müssen die Thin Clients also lediglich registrieren, um sie automatisch bereits vorab erstellten Profilen zuzuweisen.

So definieren Sie Regeln für Vorgabeverzeichnisse:

1. Wählen Sie **Extras→Vorgabeverzeichnisse**.

   Im Pop-up-Dialog wird die Liste der bereits definierten Regeln angezeigt.
2. Klicken Sie **Hinzufügen**, **Bearbeiten** und **Entfernen**, um eine neue Regel hinzuzufügen bzw. eine vorhandene Regel zu ändern oder zu löschen.
3. Klicken Sie die Schaltflächen nach oben bzw. nach unten, um die Reihenfolge der Regeln zu ändern.
4. Klicken Sie **Regeln jetzt anwenden...**, um die markierten Regeln sofort auszuführen.
5. Klicken Sie **Speichern**, um die Änderungen zu übernehmen.

> Die Reihenfolge der Regeln ist wichtig, weil die erste von einem Thin Client erfüllte Regel das Verzeichnis bestimmt, in welches der Thin Client abgelegt wird.

Verzeichnisregel erstellen/bearbeiten

1. Klicken Sie **Hinzufügen** unter **Extras→Vorgabeverzeichnisse**, um eine neue Regel zu erstellen.

   Klicken Sie **Bearbeiten** unter **Extras→Vorgabeverzeichnisse**, um eine bestehende Regel zu verändern.
2. Wählen Sie das Verzeichnis aus, in das die Thin Clients abgelegt werden sollen, wenn sie der Regel entsprechen.
3. Aktivieren Sie die Option **Überschreibt bestehende Verzeichniszugehörigkeit**, um einen bereits registrierter Thin Client im Zielverzeichnis neu zu registrieren.
4. Aktivieren Sie die Option **Regel anwenden, wenn der TC gebootet wird**, um einen bereits registrierten Thin Client auch ohne Neuregistrierung entsprechend der Verzeichnisregel nach jedem Neustart in das dazugehörige Verzeichnis zu verschieben.

Bedingungen festlegen

Mit Hilfe des Assistentendialogs legen Sie in drei Schritten die Bedingungen fest, die für die Anwendung der Regel erfüllt sein müssen.

1. Wählen Sie einen Suchparameter bzw. ein Selektionskriterium aus.

Die verfügbaren Kriterien sind:

- IP-Adresse
- Name des Thin Clients
- Netzwerkname
- Produktname
- Produkt-ID
- Firmwareversion
- Netzmaske

2. Legen Sie den Vergleichswert für das Kriterium fest.

   Die Eingabebereiche variieren je nach dem gewählten Kriterium. Weitere Informationen zu den verschiedenen Eingabebereichen finden Sie unter **Suche**.

3. Klicken Sie **Weiter**, um fortzufahren.

   Sie erhalten eine Übersicht des definierten Vorgabeverzeichnisses.

4. Aktivieren Sie die Option **Suche weiter einschränken** oder **Weiteres Auswahlkriterium festlegen**, um die Regel genauer zu definieren.

   Der Assistent öffnet erneut das Fenster **Suchparameter auswählen**.

5. Wiederholen Sie Schritt 1 bis 3.

6. Klicken Sie **Fertig**.

   Die neue Regel wird angelegt und in der Liste angezeigt.



Abbildung 18: Verzeichnisregel erstellen

Verzeichnisregel anwenden

Die Regeln können unabhängig vom Import neuer Clients oder vom Booten bestehender Clients angewendet werden:

➢ Klicken Sie **Anwenden** in der Übersicht der Verzeichnisregeln.

Dabei können Sie definieren, wie Thin Clients behandelt werden sollen, die keine der Regeln erfüllen. Sie können sie im aktuellen Verzeichnis belassen oder in einem bestimmten anderen Ordner sammeln.

Beispiele

Erstes Beispiel:

Verzeichniszuordnung über Gerätedaten

Ein Thin Client erfüllt diese Regel, wenn es sich um ein Gerät des Typs UD3 mit einer Firmware-Version höher als 4.0 handelt und die IP-Adresse aus dem Bereich 10.201.0.x stammt.

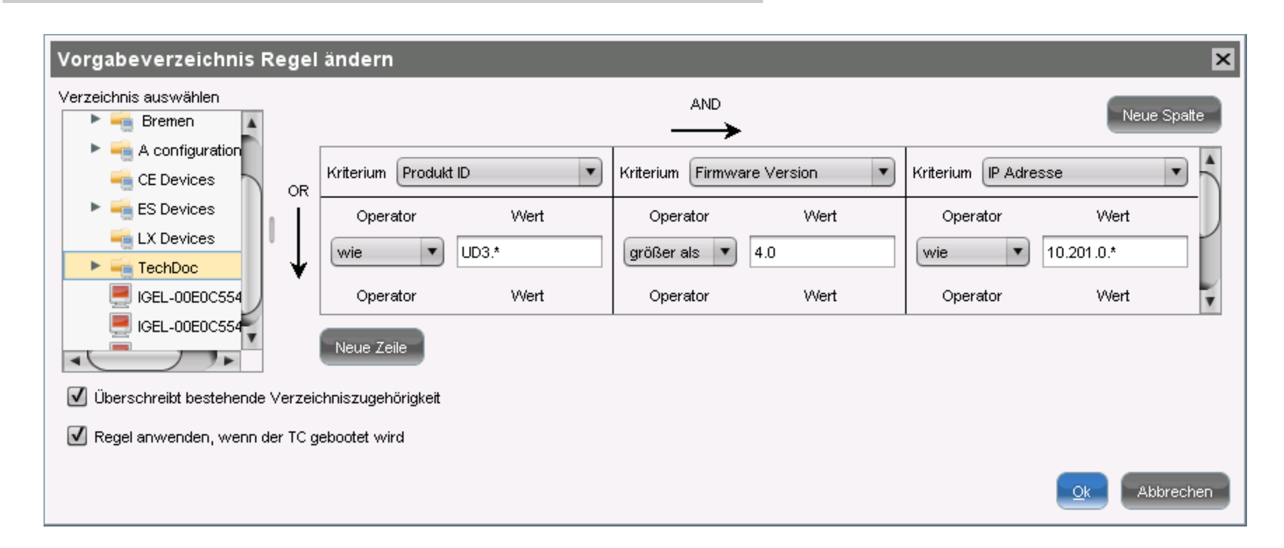


Abbildung 19: Vorgabeverzeichnisregel ändern

Zweites Beispiel:

Verzeichniszuordnung über Netzmasken

Wenn ein Thin Client in der IGEL UMS registriert wird, wird er in einen Ordner verschoben, der durch das Kriterium Netzmaske bestimmt wird. Wenn der sich daraus ergebende Ordner nicht existiert, wird er angelegt. Da diese Regel immer zutrifft, ist es nicht sinnvoll, eine weitere Regel zu definieren. Nur die erste getroffene Regel greift. Wenn die Netzmaskenregel alle Thin Clients in Verzeichnisse sortiert, ist keine weitere Regel aktiv. Der sich ergebende Ordner wird durch diese Operation ermittelt:

```
Ordner = IP Adresse AND Netzmaske
```

IP-Adresse	Netzmaske	Resultierendes Verzeichnis
130.094.122.195	255.255.255.224	130.094.122.192
172.16.232.15	255.255.0.0	172.16.0.0
192.168.1.1	255.255.255.0	192.168.1.0

Sonderfall Strukturtag

Ein besonderes Auswahlkriterium für Verzeichnisregeln ist das **Strukturtag**. Ein solches Kennzeichen kann sowohl lokal am Thin Client vergeben, als auch über DHCP jedem Thin Client zugeordnet werden. Wird ein Thin Client registriert und liefert ein solches Strukturtag, kann er durch eine Verzeichnisregel im vorgesehenen Verzeichnis abgelegt werden. Anders als bei "normalen" Verzeichnisregeln, erfasst die Regel mit Strukturtags aber mehrere Verzeichnisse gleichzeitig - das macht diese Lösung gleichzeitig flexibler und übersichtlicher und unterstützt den automatischen Roll-Out von Thin Clients optimal.

Ein Best-Practice-Dokument zur Verwendung der Strukturtags finden Sie *hier* (*http://edocs.igel.com/index.htm#10202089.htm*).

Voraussetzungen:

Damit ein Thin Client die Information zur Ablage in ein bestimmtes Verzeichnis liefern kann, sind folgende Voraussetzungen zu erfüllen.

- IGEL UMS 4.08.100 oder neuer
- Client mit IGEL Linux 5.05.100 oder neuer
- Strukturtag wird dem Client manuell oder per DHCP zugewiesen

Zuweisung eines Strukturtags an den Thin Client:

- Automatisch per DHCP: Verwenden Sie die Option 226 Ihres DHCP-Servers, um die Thin Clients im Netzwerk mit den gewünschten Strukturtags zu versorgen. Der Client reicht das Tag dann seiner Registrierung an den UMS Server weiter.
- Manuell am Thin Client: Bei der manuellen Registrierung vom Thin Client aus können Sie auch das Strukturtag dieses Clients vergeben. Siehe *IGEL Linux Fernadministration* (*http://edocs.igel.com/manuals/de/de_udlx_v5/index.htm#2694.htm*).

5.2. Thin Clients konfigurieren

Konfigurieren Sie einen Thin Client

- lokal am Gerät
- über den Konfigurationsdialog der UMS
- über ein *Profil* (Seite 62) der UMS

  oder
- per *VNC* (Seite 53)-Zugriff

So können Sie die Thin Client-Konfiguration lokal im Setup des Clients oder auch direkt für diesen Client in der IGEL UMS bearbeiten:

➢ Doppelklicken Sie den Thin Client im Navigationsbaum

  oder wählen Sie **Konfiguration bearbeiten** aus dem Menü / Kontextmenü
  oder wählen Sie das entsprechende Symbol aus der Symbolleiste.

Der Setupdialog des Thin Clients in der UMS und die Konfiguration eines Profils entsprechen dem Aufbau der lokalen Setupanwendung. Details hierzu sind im zugehörigen Systemhandbuch beschrieben.

So bestimmen Sie, wann die Konfigurationsänderungen wirksam werden sollen:

1. Ändern Sie die Konfiguration.
2. Klicken Sie **Speichern**.
3. Wählen Sie aus, wann die Einstellungen wirksam werden sollen.
   - **Nächster Neustart**: Der Thin Client ruft seine Einstellungen bei jedem Start automatisch ab.
   - **Sofort**: Die Einstellungen werden umgehend an den Thin Client übertragen.

   Wenn der Thin Client nicht in Betrieb ist, kann diese Operation nicht ausgeführt werden, und der Thin Client erhält seine Einstellung beim nächsten Neustart. In beiden Fällen werden die Einstellungen zunächst in der Datenbank gespeichert.

> Wenn Sie **Sofort** gewählt haben, wird der Benutzer des Thin Clients in einem Pop-up-Dialog gefragt, ob die neuen Einstellungen sofort wirksam werden sollen. Sie können die Benutzerabfrage ändern mit den beiden Registry-Parametern: `userinterface.rmagent.enable_usermessage` und `userinterface.rmagent.message_timeout`.

5.3. Spiegeln (VNC)

Mit der IGEL UMS-Konsole können Sie den Desktop eines Thin Clients durch Spiegeln mit VNC auf Ihrem lokalen PC beobachten. Um die Spiegelung zu aktivieren, müssen Sie in den Sicherheitsoptionen des Thin Clients den Fernzugriff zulassen.

5.3.1. VNC-Sitzung starten

So starten Sie eine VNC-Sitzung:

1. Klicken Sie im Kontextmenü eines Thin Clients auf **Spiegeln.**

   Ein Verbindungsdialog öffnet sich, die Daten des Thin Clients (IP-Adresse, Port) sind bereits vorgegeben.
2. Geben Sie das Passwort ein, wenn Sie in den Sicherheitsoptionen ein Passwort festgelegt haben.

5.3.2. IGEL VNC-Viewer

Wenn Sie die VNC-Sitzung gestartet haben, wird der gespiegelte Desktop im Fenster IGEL VNC-Viewer angezeigt. Dieses Fenster verfügt über ein eigenes Menü mit den folgenden Elementen:

Datei	**Übersicht**	Zeigt eine Übersicht aller derzeit verbundenen VNC-Sitzungen an. Doppelklicken Sie auf einen der angezeigten Desktops, um ihn in voller Größe darzustellen.
	Beenden	Beendet alle VNC-Sitzungen und schließt das Fenster.
Tab	**Neu**	Öffnet den Verbindungsdialog, sodass Sie eine weitere VNC-Sitzung starten können.
	Anpassen	Mit dieser Option können Sie die Größe des Fensters anpassen, in dem der derzeit ausgewählte Desktop angezeigt wird.

Strg-Alt-Entf senden	Sendet die Tastenkombination Strg+Alt+Entf an den derzeit angezeigten Remote Host.
Erneuern	Aktualisiert den Fensterinhalt.
Screenshot	Schreibt einen Screenshot des Fensterinhalts auf die lokale Festplatte.
Optionen	Öffnet ein Dialogfenster, in dem Sie weitere Optionen festlegen können, wie Kodierung, Farbtiefe, Aktualisierungsintervall etc.
Schließen	Schließt die derzeit ausgewählte Registerkarte.
Hilfe / Info	Zeigt die Softwareversion vom IGEL VNC-Viewer an.

Folgende Parameter können Sie als Optionen angeben:

Bevorzugte Kodierung	Die für Imagedaten beim Senden vom Thin Client zu Ihrem PC verwendete Kodierung. Die Kodierungsoption **Tight** ist besonders in einem Netzwerk mit geringer Bandbreite sinnvoll. Sie beinhaltet zwei zusätzliche Parameter: • **Kompressionsstufe**: Je höher die Komprimierung, umso länger dauert der Rechenvorgang! • **JPEG-Qualität**: Wenn Sie **aus** wählen, werden keine JPEG-Daten versendet.
Zeichne-Rechteck-Methode verwenden	Diese Option verbessert die Leistung. Es können jedoch Artefakte auftreten.
Farbtiefe	8 oder 24 Bit pro Pixel
Aktualisierungsperiode	Zeitspanne zwischen zwei Updates. Eine längere Zeitspanne verringert den Netzwerkverkehr, aber das Update verläuft dann möglicherweise nicht nahtlos. Beachten Sie: Sobald Sie die Maus bewegen oder einen Schlüssel im VNC-Viewer eingeben, wird sofort eine Updateanfrage gesendet. Dieses Ereignis wird an den Remote Host weitergegeben.
Eigenschaften als Standard speichern	Speichert die aktuellen Einstellungen als Standardwerte für zukünftige VNC-Sitzungen.

5.3.3. Externe VNC-Viewer

Sie können in der UMS-Konsole ein externes VNC-Viewer-Programm eines anderen Anbieters angeben:

➢ Klicken Sie **Extras→Einstellungen→Allgemein**.

Um die IP-Adresse des Thin Clients an eine externe Anwendung zu übermitteln, fügen Sie in **Externer VNC-Viewer** dem Programmaufruf die Parameter `<hostname>` und `<port>` hinzu.

Beispiele:

- TightVNC: `"C:\Program Files\TightVNC\tvnviewer.exe" <hostname>:<port>`
- UltraVNC: `"C:\Program Files\uvnc\UltraVNC\vncviewer.exe" -connect <hostname>::<port>`
- RealVNC: `"C:\Program Files\RealVNC\VNC Viewer\vncviewer.exe" <hostname>:<port>`
- TigerVNC: `"C:\Program Files\TigerVNC\vncviewer.exe" <hostname>:<port>`

> Setzen Sie den Programmpfad wie oben gezeigt in doppelte Anführungszeichen, damit der Aufruf auch trotz Leerzeichen im Pfad funktioniert.

5.3.4. Sicheres Spiegeln (VNC mit SSL)

Die Funktion Sicheres Spiegeln erhöht die Sicherheit bei der Fernwartung eines Thin Clients über VNC an mehreren Stellen:

- Verschlüsselung: Die Verbindung zwischen dem spiegelnden Rechner und dem gespiegelten Thin Client wird verschlüsselt.

  Dies ist unabhängig vom verwendeten VNC-Viewer.

- Integrität: Nur Thin Clients in der UMS-Datenbank können gespiegelt werden.
- Autorisierung: Nur autorisierte Personen (UMS-Administratoren mit ausreichender Berechtigung) können Thin Clients spiegeln.

  Ein direktes Spiegeln ohne Anmeldung an der UMS ist nicht möglich.

- Limitierung: Nur das in der UMS konfigurierte VNC-Viewer-Programm (interner oder externer VNC-Viewer) kann zum Spiegeln verwendet werden.

  Das direkte Spiegeln eines Thin Clients durch einen anderen Thin Client wird ebenfalls unterbunden.

- Protokollierung: Verbindungen, die über das sichere Spiegeln aufgebaut werden, werden am UMS-Server im Log erfasst.

  Zusätzlich zu den Verbindungsdaten lassen sich auch die zugehörigen Benutzerdaten (spiegelnder UMS-Administrator, optional) im Log erfassen.

> Dies alles betrifft natürlich nur Thin Clients, welche die Voraussetzungen für sicheres Spiegeln erfüllen und die entsprechende Option auch aktiviert haben. Andere Thin Clients lassen sich wie gehabt "frei" spiegeln, ggf. abgesichert durch die Abfrage eines Passworts. Möchten Sie ausschließlich sicheres Spiegeln erlauben, können Sie das in *Zusätzliche Einstellungen* (Seite 126) im Administrationsbereich festlegen.

Grundlagen und Voraussetzungen

Die Option Sicheres Spiegeln ist unter folgenden Voraussetzungen aktivierbar:

- IGEL Universal Desktop Linux oder IGEL Universal Desktop OS 2 jeweils ab Version 5.03.190 bzw. IGEL Universal Desktop Windows Embedded Standard 7 ab Version 3.09.100
- IGEL Universal Management Suite ab Version 4.07.100
- Thin Client ist am UMS-Server registriert
- Thin Client kann mit UMS-Konsole und UMS-Server kommunizieren (s.u.)

Technische Grundlagen:

Im Gegensatz zum "normalen" Spiegeln wird beim sicheren Spiegeln die Verbindung zwischen VNC-Viewer und VNC-Server (auf dem Thin Client) nicht direkt aufgebaut, sondern läuft über zwei Proxies - einen seitens der UMS-Konsole und einen seitens des VNC-Servers auf dem Thin Client. Diese Proxies kommunizieren über einen SSL-verschlüsselten Kanal, während die lokale Kommunikation z.B. zwischen VNC-Viewer-Anwendung und UMS-Proxy herkömmlich unverschlüsselt erfolgt. Somit kann eine gesicherte Verbindung auch mit externen VNC-Programmen aufgebaut werden, die selbst keine SSL-Verbindung unterstützen.

Die beiden Proxies (UMS-Konsole und Thin Client) kommunizieren SSL-verschlüsselt über den gleichen Port wie die "normale" VNC-Verbindung: 5900. Somit müssen für das sichere Spiegeln keine gesonderten Regeln für Firewalls konfiguriert werden.

Ist das sichere Spiegeln für einen Thin Client aktiv (**Setup→System→Spiegeln→Sicheres Spiegeln**), generiert der Thin Client beim nächsten Systemstart ein Zertifikat nach X.509-Standard und übermittelt dieses an den UMS-Server. Dieser überprüft spätere Anfragen nach einer sicheren VNC-Verbindung anhand des Zertifikats. Das Zertifikat liegt im PEM-Format vor im Verzeichnis `/wfs/ca-certs/tc_ca.crt` auf dem Thin Client. Die Gültigkeit des Zertifikats lässt sich am (Linux) Thin Client prüfen mit dem Kommando:
`x11vnc -sslCertInfo /wfs/ca-certs/tc_ca.crt`

```
VNC Certificate file:
        /wfs/ca-certs/tc_ca.crt

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1572055243 (0x5db3a8cb)
    Signature Algorithm: md5WithRSAEncryption
        Issuer: C=DE, L=Bremen, O=IGEL
        Validity
            Not Before: Jun  6 06:04:50 2014 GMT
            Not After : Jun  6 06:04:50 2037 GMT
        Subject: C=DE, L=Bremen, O=IGEL
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:a4:e4:67:f3:cf:23:90:06:c3:d6
                    5e:0e:00:b8:43:14:6d:61:c5:65:ca
```

Abbildung 20: Thin Client Zertifikat für sicheres Spiegeln

Ruft ein UMS-Administrator in der UMS-Konsole für den Thin Client die Funktion **Spiegeln** auf, so erhält die Konsole vom UMS-Server eine signierte Anfrage, welche dann an den zu spiegelnden Thin Client weitergeleitet wird. Dieser wiederum leitet die Anfrage erneut an den UMS-Server weiter, der Anhand des ursprünglichen Zertifikats die Gültigkeit der Anfrage prüft und im Erfolgsfall der Konsole zurückmeldet, dass der Kanal für die Verbindung zwischen den Proxies aufgebaut werden kann. Der UMS-Proxy auf der Konsole verbindet sich zum Server-Proxy auf dem Thin Client, dieser wiederum baut auf dem Thin Client die Verbindung zu dessen VNC-Server auf.

Erst wenn diese Verbindungen aufgebaut sind, ruft die Konsole den VNC-Viewer auf, der sich mit dem Proxy der Konsole verbindet. Nun sind VNC-Client und VNC-Server über die beiden Proxies verbunden, die über SSL verschlüsselt übertragen.

> Das sichere Spiegeln kann unabhängig von der Thin Client Konfiguration für alle Thin Clients erzwungen werden, die diese Funktion unterstützen: **UMS Administration > Zusätzliche Einstellungen > Sicheres VNC global aktivieren**.

Thin Clients sicher spiegeln

Um einen Thin Client sicher (verschlüsselt) zu spiegeln, muss der Administrator sich über die UMS-Konsole am Server anmelden. Dabei ist es egal, ob ein rein lokales UMS-Administratorkonto verwendet wird oder der Benutzer z.B. über ein Active Directory übernommen wurde. Der UMS-Administrator muss aber wie üblich über das Recht zum Spiegeln des Objekt besitzen:

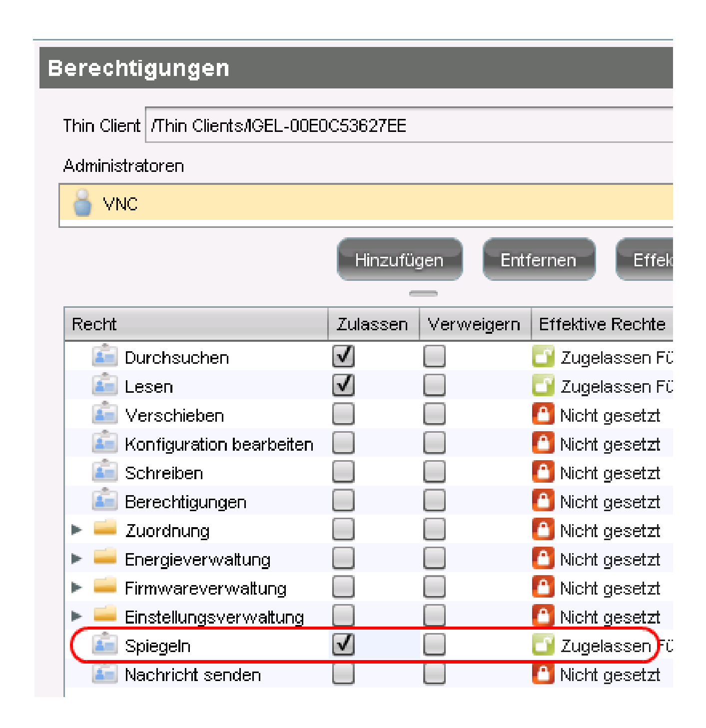


Abbildung 21: Administratorrecht Spiegeln

Der zu spiegelnde Thin Client wird im Navigationsbaum aufgerufen und wie üblich kann über das Kontextmenü der Punkt **Spiegeln** ausgeführt werden. Das Verbindungsfenster unterscheidet sich jedoch vom Dialog des normalen VNC-Spiegelns. Weder lassen sich IP und Port des zu spiegelnden Thin Clients ändern, noch wird ein Passwort für die Verbindung abgefragt - dies ist durch die zuvor erfolgte Konsolenanmeldung überflüssig.



Abbildung 22: Verbindungsdialog Sicheres Spiegeln

Bei bestehender VNC-Verbindung erkennt man das sichere Spiegeln am Symbol des Verbindungsreiters:



Abbildung 23: Sichere VNC-Verbindung

VNC-Logging

Verbindungen über das sichere Spiegeln werden grundsätzlich in der UMS protokolliert. Dabei lässt sich in **UMS-Administration→Zusätzliche Einstellungen→Sichere VNC-Verbindung** konfigurieren, ob der Benutzername des Spiegelnden in das Log aufgenommen werden soll (Vorgabe ist inaktiv):

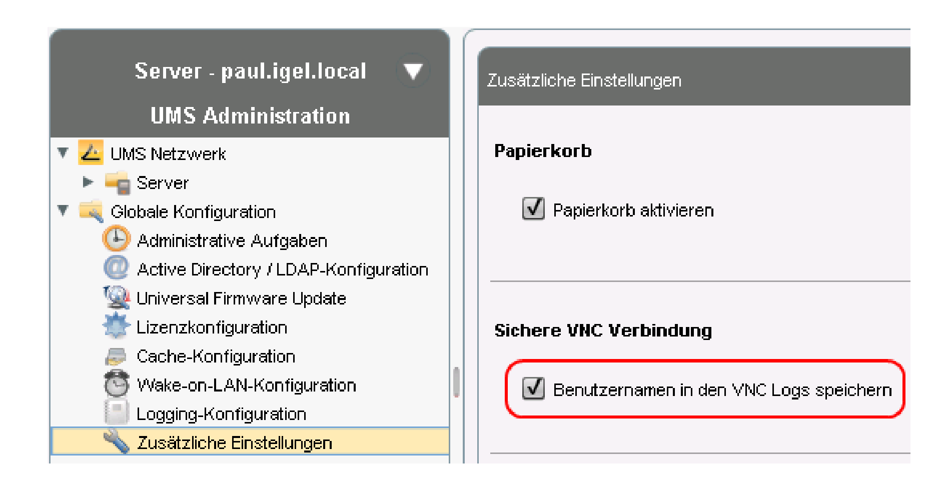
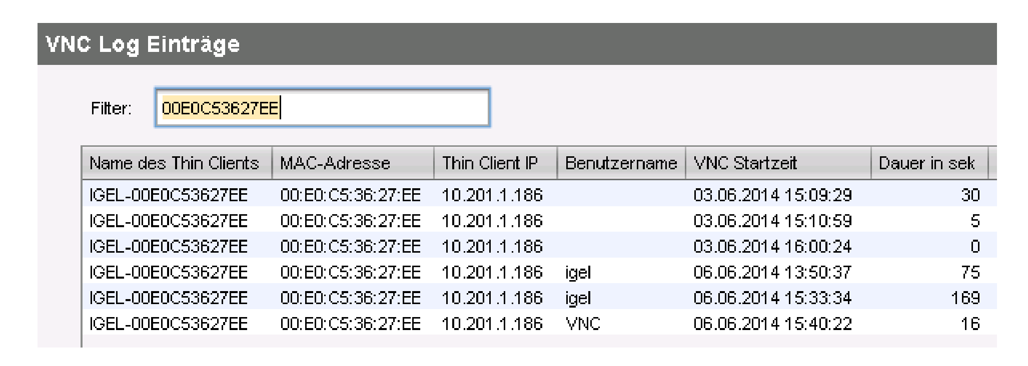


Abbildung 24: Optionen für VNC-Logging

Das VNC-Log lässt sich über das **Kontextmenü** eines Thin Clients oder eines Ordners (für mehrere Thin Clients) aufrufen (**Logging→VNC-Log**). Protokolliert werden Name, MAC-Adresse und IP-Adresse des gespiegelten Thin Clients, Zeitpunkt und Dauer des Vorgangs und ggf. der Benutzername des spiegelnden UMS-Administrators:



VNC Log Einträge

Filter: 00E0C53627EE

Name des Thin Clients	MAC-Adresse	Thin Client IP	Benutzername	VNC Startzeit	Dauer in sek
IGEL-00E0C53627EE	00:E0:C5:36:27:EE	10.201.1.186		03.06.2014 15:09:29	30
IGEL-00E0C53627EE	00:E0:C5:36:27:EE	10.201.1.186		03.06.2014 15:10:59	5
IGEL-00E0C53627EE	00:E0:C5:36:27:EE	10.201.1.186		03.06.2014 16:00:24	0
IGEL-00E0C53627EE	00:E0:C5:36:27:EE	10.201.1.186	igel	06.06.2014 13:50:37	75
IGEL-00E0C53627EE	00:E0:C5:36:27:EE	10.201.1.186	igel	06.06.2014 15:33:34	169
IGEL-00E0C53627EE	00:E0:C5:36:27:EE	10.201.1.186	VNC	06.06.2014 15:40:22	16

Abbildung 25: Logeinträge der sicheren VNC-Verbindungen

- Klicken Sie zum Sortieren der Liste (z.B. nach Benutzername) auf die entsprechende **Spaltenüberschrift** oder filtern Sie die angezeigten Inhalte durch Eingaben im Feld **Filter**.

5.4. Firmware Lizenzen

IGEL Thin Clients der Produktreihe Universal Desktop (z. B. UD5) werden mit installierter Lizenz ausgeliefert. Diese Lizenz ermöglicht die Nutzung verschiedener Firmwarefunktionen und ist mit der MAC-Adresse des Thin Clients verbunden. Manuell erstellte Thin Clients oder per UDC2 "konvertierte" Hardware von Fremdherstellern haben u.U. keine Lizenz. Deshalb muss die Lizenz später zur Firmware hinzugefügt werden. Auch Upgrade-Lizenzen können nachträglich über die Lizenzverwaltung der UMS ausgerollt werden.

5.4.1. Lizenzverwaltung

Über **System→Lizenzen verwalten** können Sie die MAC-Adressen aller Thin Clients, aller unlizenzierten Thin Clients oder der über eine View selektierten Thin Clients in eine `CSV`-Datei exportieren. Diese Datei kann an die IGEL Technology GmbH gesendet werden, um eine Lizenzdatei für diese Geräte anzufordern.

Die erhaltene Lizenzdatei kann über die Schaltfläche **Hinzufügen (+)** in der Lizenzverwaltung hinzugefügt werden. Die Lizenz wird beim nächsten Startvorgang an die zuvor ausgewählten Thin Clients verteilt.

> Der Thin Client muss den UMS-Server mit seinem Full-Qualified-Domain-Namen, wie z. B. `mytcserver.mydomain.tld`, kontaktieren können.

5.4.2. UDC2-Testlizenzen

Wenn Sie IGEL Universal Desktop Converter 2 (UDC2) testen, verwenden Sie bitte den normalen Lizenzmechanismus. UDC2-Testlizenzen sind bereits mit Ihrer Hardware verbunden, welche durch deren MAC-Adresse repräsentiert wird.

5.4.3. UDC2-Lizenzen verteilen

Der IGEL Universal Desktop Converter 2 umfasst einen USB-Token mit dem IGEL Universal Desktop OS 2 sowie eine SIM-Karte mit den Lizenzen, die Sie für die Ausführung dieser Firmware auf dem Zielsystem benötigen.

Installieren Sie das IGEL Universal Desktop OS 2 auf dem Zielsystem (siehe IGEL UDC2 Installationshandbuch) und lizenzieren Sie diese Software

- durch Erstellen einer Lizenz während der Installation, oder
- durch das Verteilen der Lizenzen auf bereits installierten Systemen mit der UMS-Lizenzverwaltung.

Voraussetzung: Das IGEL Universal Desktop OS 2 ist auf den Zielgeräten installiert und die Geräte sind auf dem UMS-Server registriert.

So erstellen Sie eine UDC2-Lizenz:

1. Legen Sie die SIM-Karte mit den Lizenzen in den Kartensteckplatz des USB-Tokens ein.
2. Stecken Sie den USB-Token in den PC ein, auf dem die UMS-Konsole installiert ist.

   Dies gilt nur bei der Windows-Version.

3. Installieren Sie bei Bedarf den Treiber für den Smartcardleser. Einen Treiber finden Sie auf dem USB-Token.
4. Starten Sie die UMS-Konsolenanwendung und navigieren Sie zu **System→Lizenzen verwalten**.

   Das neue Fenster zeigt Lizenzinformationen an.

5. Klicken Sie auf **Lizenzen von der Smartcard ausstellen** und bestätigen Sie den Prozessstart.

   Die Anzahl der verfügbaren Lizenzen und der Typ werden angezeigt.

6. Wählen Sie aus den unlizenzierten Geräten diejenigen aus, für die eine Lizenz erstellt werden soll.

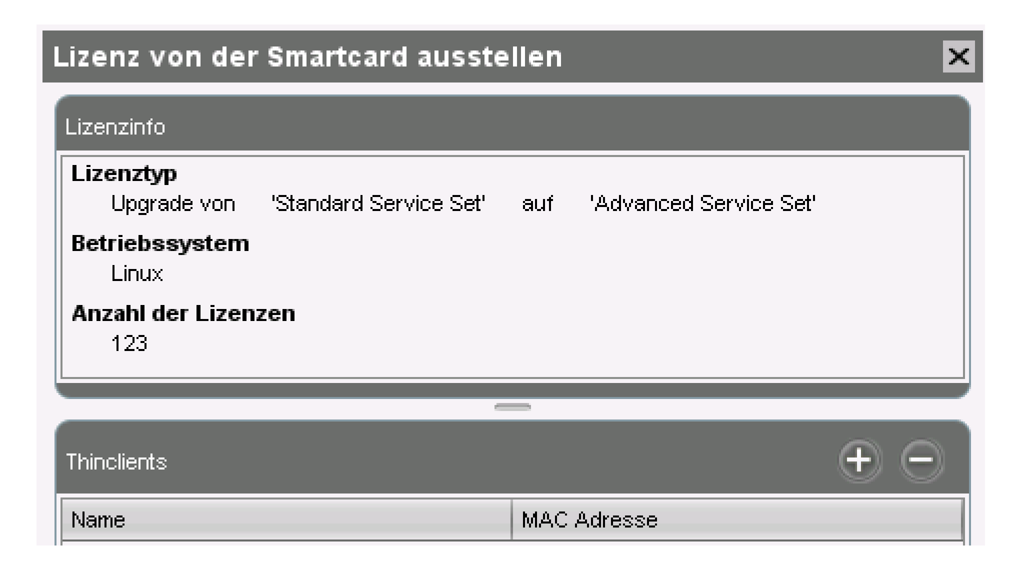


Abbildung 26: Lizenzen von der IGEL-Smartcard ausstellen

Eine Lizenz wird aus dem Lizenzpool auf dem Stick erstellt. Nach zweimaligem Neustart verfügt das Gerät über die Funktionen, die der Lizenz entsprechen.

Sie können stattdessen auch UMS-Einstellungen an die UDC2-Geräte senden, um die Lizenz zu übertragen. Starten Sie die Geräte neu, um die neue Lizenz zu aktivieren.

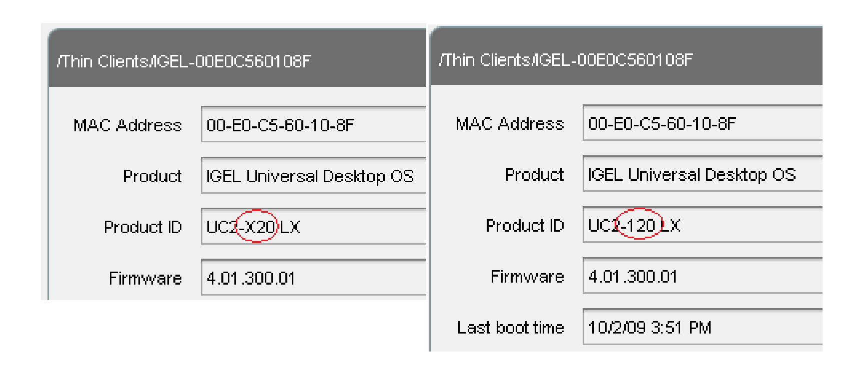


Abbildung 27: Lizenzverwaltung

- Überprüfen Sie, ob das Gerät die Lizenz richtig verwendet hat. Die Produkt-ID sollte sich von `X20` auf `120`, `520` oder `720` geändert haben. Dies ist vom Lizenztyp Entry, Standard oder Advanced abhängig.

  Zusätzlich werden jetzt die mit IGEL UMS lizenzierten IGEL-Thin Clients und UDC2-Geräte im Dialog der Lizenzverwaltung angezeigt.

Aus dem Lizenzpool erstellte Lizenzen werden auf dem Token gespeichert, sodass Sie sie wiederverwenden können, falls Sie die IGEL-Firmware erneut auf dem Gerät installieren müssen.

5.4.4. Upgrade von Lizenzen

Für das Upgrade der Lizenz eines UD-Geräts, also UD-Thin Client oder UDC2, auf ein höheres Feature Set wenden Sie den gleichen Mechanismus mit USB-Token und SIM-Karte an, wie bei den UDC2-Lizenzen.

Auf einer SIM-Karte verfügbare Upgradelizenzen werden mit ihrem Lizenztyp angezeigt, z. B. **Entry auf Advanced**. In der Geräteauswahl werden nur geeignete Geräte aufgeführt, z. B. Thin Clients mit dem **UDLX Entry Feature Set**.

6. Profile

Profile sind vordefinierte Konfigurationen, die global über die Universal Management Suite Verzeichnissen, Gruppen, Benutzern oder Thin Clients zugewiesen werden können. Folgende verschiedene Typen gibt es:

Standardprofile	...können Objekten (Thin Clients oder Benutzer) direkt oder indirekt über Verzeichnisse zugeordnet werden. Ein Objekt kann seine Einstellungen von mehreren direkt oder indirekt zugewiesenen Profilen bekommen. Bei der Zuweisung überschreiben die Profileinstellungen die direkt am Thin Client vorgenommenen Einstellungen.
Masterprofile (Seite 78)	...erlauben eine flexiblere Gestaltung der Zugriffsrechte innerhalb der IGEL UMS, indem sie Einstellungen von Standardprofilen übersteuern können und eigene Berechtigungen besitzen. Diese verschiedenen Profiltypen lassen sich miteinander kombinieren.

Besondere Profilausprägungen

Benutzerprofile (Seite 71)	Standard- und Masterprofile können Active Directory-Benutzern zugeordnet werden und erlauben damit: • Shared Workplace: Wechselnde Benutzer an einem Arbeitsplatz • Roaming Doctors: Wechselnde Arbeitsplätze eines Benutzers
Templateprofile (Seite 83)	Mittels dynamisch ermittelter Werte lassen sich Standard- und Masterprofile noch flexibler einsetzen und kombinieren.

6.1. Rangfolge der Einstellungen

Durch ein Profil gesetzte Parameter sind im Konfigurationsdialog des Thin Clients gesperrt und mit einem Schlosssymbol gekennzeichnet.

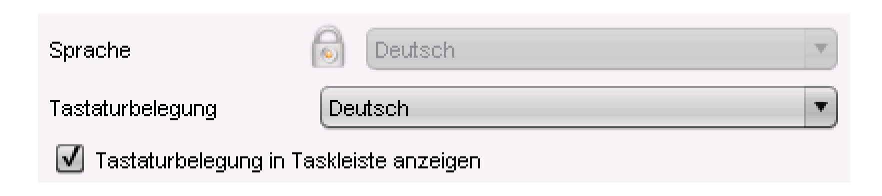


Abbildung 28: Einstellung mit Schlosssymbol

Sie können nur im Profil bearbeitet werden. Der Name des sperrenden Profils wird angezeigt, wenn Sie mit dem Mauszeiger über dem Schlosssymbol verweilen.

Jeder Parameter verfügt über zwei Wertetypen:

- die durch den Thin Client bestimmten Werte und
- die durch die Profile bestimmten Werte.

Sie existieren parallel, und es gilt die Regel, dass die Profileinstellungen immer Vorrang haben.

Wenn Sie in einem Profil einen Wert für einen Parameter gesetzt haben und die Zuweisung zu einem Thin Client aufheben, wird der Wert des Parameters in seinen vorherigen Thin Client-Wert geändert. Der Profilwert wird nicht in die Thin Client-Einstellungen kopiert.

6.2. Rangfolge der Profile

Wenn Sie einem Thin Client mehrere Profile zugewiesen und eine bestimmte Einstellung in allen Profilen aktiviert haben, möchten Sie vielleicht wissen, welches Profil den geltenden Wert für diese Einstellung liefert oder mit anderen Worten, welches Profil Vorrang vor den anderen hat.

Versuchen Sie es zu vermeiden, gleiche Einstellungen in mehreren Profilen zu aktivieren, indem Sie getrennte Gruppen aktiver Parameter für unterschiedliche Profile einrichten. Sonst gilt folgende symbolische Regel:

Je näher ein Objekt, dem das Profil zugewiesen wurde, dem Thin Client ist, umso höher ist die Position des Profils in der Rangfolge.

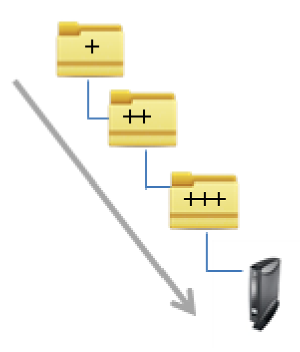


Abbildung 29: Die Priorität der Standardprofile nimmt mit jeder Ebene zu

Höhere Priorität	als...
näher am Thin Client	weiter weg vom Thin Client
Unterverzeichnis	übergeordnetes Verzeichnis

Wenn einem Verzeichnis mehrere Profile zugewiesen sind bzw. mehrere Profile direkt zugewiesen werden, überschreibt das neuere Profil, mit der höheren Profil-ID, die Einstellungen.

Um die ID eines Profils auszulesen, zeigen Sie mit dem Mauspfeil auf ein Profil in der Liste der zugewiesenen Profile. Es wird ein Tooltip mit der Profil-ID angezeigt.

Die Listen der zugewiesenen Profile und der indirekt zugewiesenen Profile sind entsprechend der Rangfolge geordnet. Bei direkten Profilen oder indirekten Profilen einer Verzeichnisebene hat also das Profil weiter oben in der Liste den höheren Rang.

6.3. Profile verwenden

In diesem Kapitel erfahren Sie, wie Sie

- *Profile erstellen* (Seite 65)
- *Profile zuweisen* (Seite 69)
- *Profile überprüfen* (Seite 70)
- *Profilzuweisung vom Thin Client entfernen* (Seite 70)
- *Sitzungen überschreiben* (Seite 69)
- *Profile exportieren und importieren* (Seite 66)
- *Profileinstellungen konfigurieren* (Seite 68)
- *Profile löschen* (Seite 71)

6.3.1. Profile erstellen

Sie haben die Grundidee von Profuilen verstanden und haben für sich ein Szenario gefunden, in dem sie Profile einsetzen möchten? Dann legen Sie los.

So erstellen Sie ein neues Profil:

1. Wählen Sie **Profil** aus dem Menü **System→Neu**,

   oder wählen Sie die entsprechende Option aus dem Kontextmenü.
   Das Dialogfenster **Neues Profil** wird angezeigt.

   > Das neue Profil wird im ausgewählten Profilverzeichnis hinterlegt. Wurde keins ausgewählt, wird es direkt im Knoten **Profile** abgelegt.

2. Geben Sie einen **Namen** für das Profil und eine **Beschreibung** ein.
3. Wählen Sie aus, ob das neue Profil Einstellungen eines vorhandenen Profils oder Thin Clients übernehmen soll.

   > Wenn Sie ein „leeres" Profil benötigen, das keine Einstellungen übernehmen soll, müssen Sie eine Firmwareversion für das neue Profil auswählen. In diesem Fall wählen Sie kein Objekt aus dem Navigationsbaum aus.

4. Wählen Sie eine der möglichen Optionen aus:
   - **Aktiviere keine Einstellungen**
   - **Aktiviere Einstellungen deren Wert vom Defaultwert abweicht**
   - **Aktiviere alle Einstellungen**
   - **Sessions überschreiben**
5. Klicken Sie **Erzeugen**, um das Profil anzulegen und zu speichern.

Neues Profil - Optionen

Die Auswahlmöglichkeiten im Fenster **Neues Profil** haben folgende Bedeutung:

Aktiviere keine Einstellungen	Zunächst sind keine Einstellungen aktiv. Konfigurieren Sie das Profil, um die gewünschten Einstellungen zu aktivieren.
Aktiviere alle Einstellungen	Alle verfügbaren Parameter des Profils werden aktiviert. Beachten Sie, dass dadurch alle Einstellungen am Thin Client mit einem Schlosssymbol gesperrt sind. Ein Profil mit dieser Einstellung setzt die Einstellungen aller anderern Profile außer Kraft und verhindert somit indirekte Einstellungszuweisungen. Diese Option ist nur in Ausnahmefällen sinnvoll. Nur wenn Sie alle Einstellungen eines Thin Clients durch dieses Profil regeln lassen möchten.
Aktiviere Einstellungen deren Werte vom Defaultwert abweichen	Diese Option ist dann von Vorteil, wenn Sie die Einstellungen eines vorkonfigurierten Thin Clients auf weitere Geräte verteilen möchten. Sie ist nur aktiv, wenn Sie vorher einen Thin Client ausgewählt haben.
Sessions überschreiben	Überschreibt die für den Thin Client definierten Sitzungen mit den Sitzungen dieses Profils. Wenn das Kontrollkästchen leer ist, werden die im Profil definierten Sitzungen zu den Sitzungen hinzugefügt, die zuvor für den Thin Client definiert wurden.

Profile, die alle Parameter einer Firmware enthalten, belegen oft unnötig Platz in Datenbanken und Backupdateien. Sie sollten diese Option nur dann verwenden, wenn es notwendig erscheint. In den allermeisten Fällen empfiehlt es sich, die Konfiguration eines Thin Clients über mehrere Profile mit spezifischen Konfigurationsteilen vorzunehmen.

Wenn noch keine Firmware in der Datenbank registriert wurde, können keine Profile erstellt werden, da Informationen zu den Einstellungen erforderlich sind, die dem Profil zugewiesen werden sollen. Sie können Profile nur mit einer Firmwareversion erstellen, die bereits in der UMS-Datenbank registriert ist.

6.3.2. Profile exportieren und importieren

In der IGEL UMS können Profilkonfigurationen aus der Datenbank in das Dateisystem exportiert werden. Dies kann für Backupzwecke oder zum Importieren der Profildaten einer UMS-Installation in eine andere hilfreich sein.

Wenn Sie über eine XML-Datei mit Profildaten oder ein ZIP-Archiv mit mehreren Profilen verfügen, können Sie diese in Ihre UMS-Installation oder in eine andere als die Ursprungsinstallation importieren.

Profil und Firmwareinformationen exportieren

> Die Profile werden in das XML-Format konvertiert. Achten Sie darauf, diese Dateien nicht zu veröffentlichen, wenn die Quellprofile Passwörter oder andere vertrauliche Daten enthalten!

So exportieren Sie ein einzelnes Profil:

1. Klicken Sie mit der rechten Maustaste auf das Profil.
2. Wählen Sie den Befehl **Exportiere Profil.**

So exportieren Sie mehrere Profile in eine Datei (ZIP-Archiv):

1. Markieren Sie die gewünschten Profile mit den Tasten Strg bzw. Umschalt.
2. Wählen Sie **System→Exportieren→Profil exportieren.**

   Das Fenster **Exportiere Profile** öffnet sich.

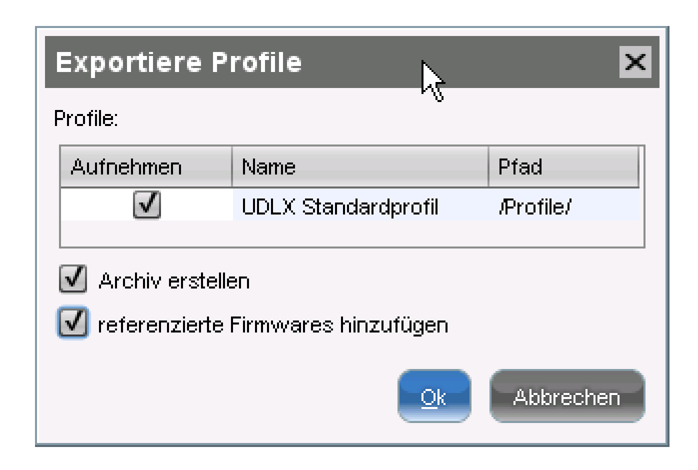


Abbildung 30: Exportiere Profile

3. Wählen Sie die Zieldatei aus.

   Beachten Sie, dass bereits vorhandene Dateien mit den neuen Profildaten überschrieben werden.

Die Firmwareinformationen lassen sich gemeinsam mit den Profildaten in ein Archiv exportieren, dies erlaubt den Import auch in eine UMS-Installation ohne passende registrierte Firmware. Diese kann nun zusammen mit dem Profil importiert werden.

Profil und Firmwareinformationen importieren

So importieren Sie ein einzelnes Profil:

1. Klicken Sie **System→Importieren→Profile importieren**.
2. Wählen Sie die XML-Datei bzw. das Archiv mit Ihrem/Ihren Profile/n aus.

   Das Dialogfenster **Profile importieren** wird geöffnet. Hier werden der Name und die Firmwareversion jeder Profilkonfiguration angezeigt, die in der von Ihnen ausgewählten Datei enthalten ist.
3. Deaktivieren Sie eins der Kontrollkästchen in der linken Reihe der Tabelle, um das zugehörige Profil vom Importprozess auszunehmen.

Beim Import lässt sich der ursprüngliche Verzeichnispfad des Profils beibehalten oder aber das Profil wird im Hauptverzeichnis abgelegt.

   Ein Dialogfenster zeigt an, ob alle gewählten Profile importiert wurden.
   Eine bisher nicht in der Datenbank vorhandene Firmwareinformation aus einem Archiv wird automatisch zusammen mit dem entsprechenden Profil importiert.

Profile mit unbekannter Firmware importieren

Ein Profil, dessen zugrundeliegende Firmwareinformation weder in der Datenbank vorhanden, noch in der Importdatei enthalten ist, kann nicht ohne Anpassungen importiert werden. Es ist in der Importansicht rot markiert.

Solche Profile können Einstellungen enthalten, die in keiner der registrierten Firmwareversionen enthalten sind.

So importieren Sie Profile, die eine unbekannte Firmware referenzieren:

1. Klicken Sie auf das rot markierte Firmwarefeld.
2. Wählen Sie eine möglichst verwandte Firmwareversion aus, die dem System bekannt ist.
3. Importieren Sie das Profil.

Wenn eine **bekannte** Firmware gewählt wird, findet eine implizite Konvertierung der Profilinformationen statt. Dies hat normalerweise kaum Auswirkungen auf die Profileinstellungen, wenn Sie eine ähnliche Firmware oder eine neuere Version des gleichen Modells auswählen. **Unbekannte** Firmwareeinstellungen gehen dabei aber verloren.

6.3.3. Profileinstellungen konfigurieren

Die Eigenschaften eines Profils bestehen aus den sogenannten Beschreibungsdaten und der Profilkonfiguration.

Beschreibungsdaten bestehen aus dem Namen des Profils, einem Beschreibungstext, der Firmwareversion und dem Überschreibungs-Flag für Sitzungen. Beispiel:

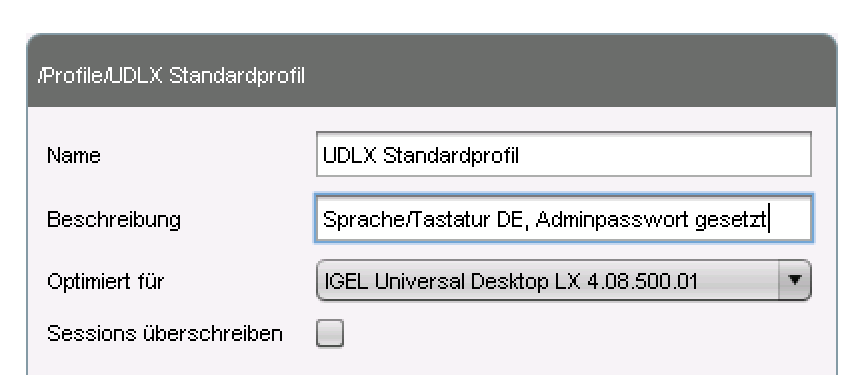


Abbildung 31: Beschreibungsdaten des Profils

➢ Klicken Sie **Bearbeiten→Beschreibungsdaten speichern** oder das Diskettensymbol in der Werkzeugleiste, um diese Daten zu speichern.

Die Daten sind nun in der Datenbank aktualisiert.

Beachten Sie bei Aktualisierungen der Firmware, dass Profileinstellungen verloren gehen, wenn sie in der neuen Firmware nicht unterstützt werden.

So bearbeiten Sie die Einstellungen eines Profils:

➢ Doppelklicken Sie ein **Profil**,

oder wählen Sie ein Profil im Navigationsbaum.

➢ Klicken Sie **Bearbeiten→Konfiguration bearbeiten**.

Die Thin Client-Setupoberfläche öffnet sich.

Blau markierte Pfade im Konfigurationsmenü führen zu Einstellungen, die bereits über das Profil gesetzt sind.

- Um Einstellungen zu ändern klicken Sie das Aktivierungssymbol vor dem Parameter, bis die gewünschte Funktion aktiv ist.

 Der Parameter ist inaktiv und wird nicht durch das Profil konfiguriert.

 Der Parameter ist aktiv und der eingestellte Wert wird durch das Profil konfiguriert, Templateschlüssel sind für den Parameter nicht verfügbar.

Beim Speichern des Profils können Sie bestimmen, wann Ihre Änderungen wirksam werden sollen:

1. Nehmen Sie die gewünschten Änderungen vor.
2. Klicken Sie **Speichern**.
3. Entscheiden Sie, ob die neuen Einstellungen sofort oder beim nächsten Start der betreffenden Thin Clients wirksam werden sollen.

6.3.4. Sitzungen überschreiben

Die Profiloption **Sitzungen überschreiben** stellt sicher, dass nur die Sitzungen dieses Profils am Thin Client angelegt werden. Sitzungen, die in anderen Profilen oder direkt in der Konfiguration des Thin Clients angelegt sind, werden unwirksam.

Sind einem Thin Client (oder Shared Workplace Benutzer) mehrere Profile mit aktivierter Option **Sitzungen überschreiben** zugewiesen (direkt oder indirekt), so "gewinnt" das Profil mit der höchsten Priorität, d.h. nur die Sitzungen dieses Profils stehen am Thin Client zur Verfügung.

Ausnahme: Ist das höchstpriorisierte Profil mit aktivierter Option ein Standardprofil und sind dem Thin Client oder dem Benutzer auch *Masterprofile* (Seite 78) mit Sitzungen zugewiesen, so erhält der Thin Client alle Sitzungen des überschreibenden Standardprofils und der Masterprofile - Sitzungen in Masterprofilen können nur durch ein Masterprofil überschrieben werden.

6.3.5. Profile zuweisen

Wenn Sie ein Profil erstellt und seine Einstellungen angepasst haben, können Sie es den Thin Clients zuweisen. Sie können jedem Thin Client eine beliebige Zahl von Profilen zuweisen.

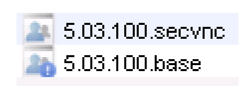
Grundsätzlich existieren zwei Zuweisungsmodi: **direkt** oder **indirekt**.

Indirekt bedeutet, dass Sie das Profil nicht einem einzelnen Thin Client sondern einem Thin Client-Verzeichnis zuweisen und alle Thin Clients in diesem Verzeichnis die Einstellungen dieses Profils übernehmen (siehe *Rangfolge der Profile* (Seite 63)).

Beachten Sie folgende Regeln:

- Wenn Sie ein Profil einem Verzeichnis zuweisen, ist es **indirekt** jedem Thin Client in diesem Verzeichnis zugewiesen, auch den Unterverzeichnissen.
- Wenn Sie einen Thin Client nachträglich in dieses Verzeichnis verschieben, wirken sich die Verzeichnisprofile auch auf diesen Thin Client aus.
- Wenn Sie einen Thin Client aus diesem Verzeichnis entfernen, beeinflusst das Profil diesen Client nicht mehr.

Zugewiesene Profile mit noch nicht an den Thin Client übertragenen Konfigurationsänderungen werden in der Liste zugeordneter Objekte mit einem Ausrufezeichen markiert:



6.3.6. Profile überprüfen

Im Bereich **Zugeordnete Objekte** können Sie zu einem zugewiesenen Thin Client, Profil oder zu einer zugewiesenen Datei navigieren oder die Konfiguration bearbeiten.

- ➢ Wählen Sie ein Objekt aus.
- ➢ Klicken Sie das Symbol **Bearbeiten**, um das Objekt zu bearbeiten.
- ➢ Klicken Sie das Symbol **Navigieren**, um im Navigationsbaum zu diesem Objekt zu navigieren.
- ➢ Doppelklicken Sie auf ein zugewiesenes Objekt, um direkt dorthin zu springen.

Wenn Sie einem Thin Client ein Profil zugewiesen haben, überprüfen Sie die Ergebnisse:

1. Wählen Sie einen Thin Client aus, und klicken Sie **Bearbeiten→Konfiguration bearbeiten**.

   Die aktuelle Konfiguration des Thin Client wird angezeigt.
   Blau markierte Pfade führen zu den Profilwerten. Vor jeder überschriebenen Einstellung wird ein Schloss angezeigt, d. h. vor einer aktiven Einstellung eines zugewiesenen Profils. Es wird der Wert angezeigt, den Sie im Profil festgelegt haben. Sie können die Einstellung hier nicht bearbeiten.

2. Fahren Sie mit der Maus über das Schlosssymbol.

   Ein Tooltip zeigt an, aus welchem Profil der Parameterwert gezogen wurde. Dies ist hilfreich, wenn Sie dem Thin Client mehr als ein Profil zugewiesen haben. Wenn eine Einstellung in mehreren zugewiesenen Profilen aktiv ist, gilt der Wert des aktuellsten Profils.

6.3.7. Profilzuweisung vom Thin Client entfernen

So können Sie die Zuordnung zwischen Profilen und Thin Clients oder einem Thin Client-Verzeichnis aufheben:

1. Markieren Sie ein Profil im Navigationsbaum.
2. Wählen Sie im Fensterbereich **Zugeordnete Objekte** einen Thin Client oder ein Thin Client-Verzeichnis aus.
3. Klicken Sie das Symbol **Entfernen**.

oder

1. Markieren Sie einen Thin Client oder ein Thin Client-Verzeichnis im Navigationsbaum.
2. Wählen Sie im Fensterbereich **Zugeordnete Objekte** ein zugewiesenes Profil aus der Liste aus.
3. Klicken Sie das Symbol **Entfernen**.

Dieses Profil hat nun keine Auswirkungen mehr auf den einzelnen Thin Client bzw. die Thin Clients im Verzeichnis. Der überschriebene Wert der Einstellungen wird auf den Wert zurückgesetzt, der vor Zuweisung des Profils gültig war.

6.3.8. Profile löschen

Wenn Sie ein Profil löschen möchten, haben Sie folgende Optionen:

1. Wählen Sie das Profil im UMS-Navigationsbaum aus.
2. Klicken Sie in der Symbolleiste auf das Symbol **Löschen**

   oder drücken Sie die Entf-Taste auf Ihrer Tastatur
   oder klicken Sie mit der rechten Maustaste auf das Profil, und wählen Sie aus dem Kontextmenü die Option **Löschen**.

Gleiches gilt auch für Verzeichnisse. Diese werden mitsamt aller Unterverzeichnisse und Profile gelöscht.

Wenn Sie ein Profil löschen, wird es für jeden Thin Client oder jedes Thin Client-Verzeichnis entfernt, dem es zugewiesen wurde. Die Werte des Profils wirken nicht mehr auf die Thin Client-Einstellungen. Außerdem werden alle Einstellungen des Profils aus der Datenbank gelöscht.

6.4. Benutzerprofile – IGEL Shared Workplace

IGEL Shared Workplace ist ein optional zu lizenzierendes Feature der IGEL Universal Desktop-Firmware und erlaubt die nutzerabhängige Konfiguration anhand von Einstellungsprofilen, die in der IGEL Universal Management Suite angelegt und mit den AD-Benutzerkonten verknüpft werden. Dabei werden benutzerspezifische Profileinstellungen mit den geräteabhängigen Parametern gemeinsam an den Thin Client übermittelt.

Eine Übersicht der für einen Benutzer individuell konfigurierbaren Parameter finden Sie *hier* (Seite 77).

Typische Beispiele für Shared Workplace bilden Schichtarbeitsplätze oder auch Callcenter, an denen verschiedene Anwender an einem Arbeitsplatz unterschiedliche Einstellungen benötigen, wie zum Beispiel Sitzungstypen oder Mauseinstellungen für Rechts- und Linkshänder.

Ein weiteres Einsatzfeld bilden Roamingumgebungen, in denen die Anwender häufig den IT-Arbeitsplatz wechseln, wie zum Beispiel in Krankenhäusern, an Schalterplätzen, Kassen oder Rezeptionen. Nach der Anmeldung des Nutzers konfiguriert sich der für Shared Workplace lizenzierte Thin Client automatisch über den UMS-Server mit dem in der UMS-Datenbank hinterlegten Einzel- bzw. Gruppenprofil. Die Zuordnung der Einstellungsprofile zum Benutzer erfolgt mithilfe der IGEL Universal Management-Konsole bequem und einfach per Drag-and-Drop.

Mit zunehmender Anzahl an Shared Workplace Arbeitsplätzen empfiehlt IGEL die Nutzung der neuen UMS High Availability Extension. Die damit erzielte Hochverfügbarkeit des UMS-Servers stellt sicher, dass Benutzer jederzeit ihr personalisiertes Profil erhalten.

Das IGEL Shared Workplace-Feature ist in der IGEL-Firmware ab Version 4.08.100 (UD-LX) bzw. 2.09.500 (UD-ES) enthalten und kann ab Version 4 der IGEL UMS genutzt werden.

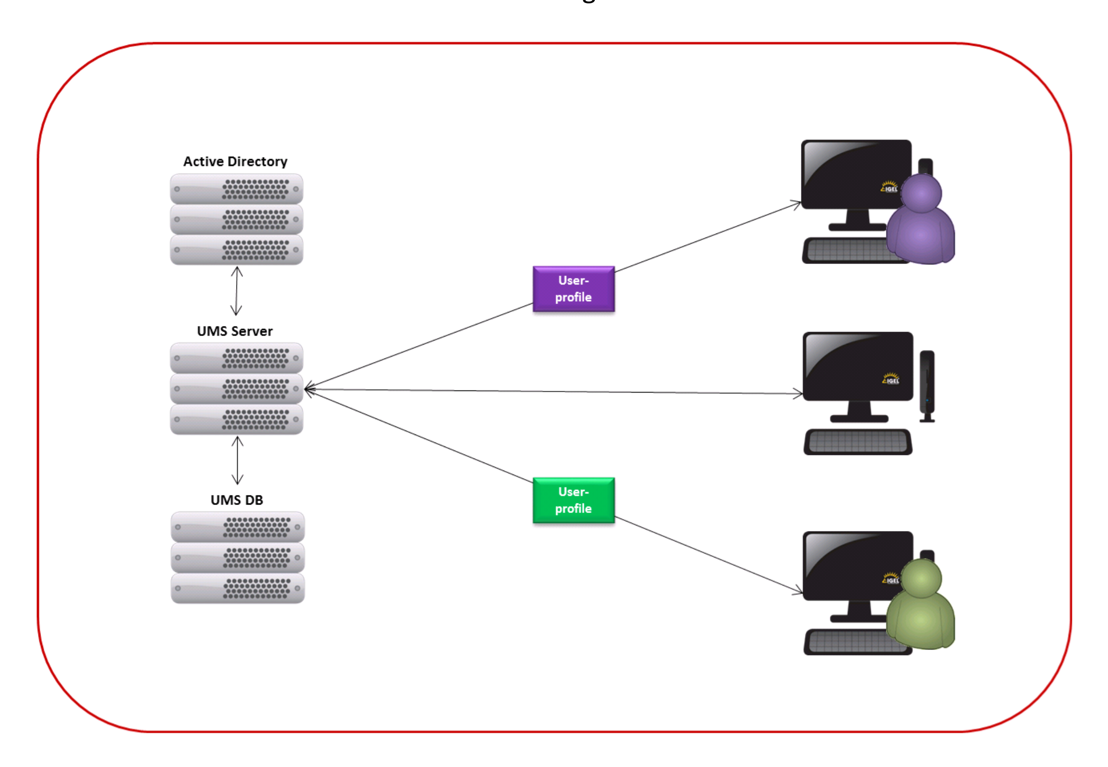


Abbildung 32: IGEL SHARED WORKPLACE-Szenario

6.4.1. Einrichtung und Verwendung

Um IGEL Shared Workplace nutzen zu können, müssen folgende Voraussetzungen erfüllt sein:

- Benutzer, die ein spezifisches Profil erhalten sollen, müssen in einem Microsoft Active Directory angelegt sein.
- Thin Clients, die eine Benutzeranmeldung erlauben sollen, müssen eine **Lizenz für die Funktion IGEL Shared Workplace** besitzen. Diese lässt sich über die Lizenzverwaltung der IGEL UMS an die Thin Clients übertragen.

  Hat ein Thin Client eine Lizenz für IGEL Shared Workplace erhalten, so kann dies nicht rückgängig gemacht werden. Die Funktion an sich kann aber über die Liste der zur Verfügung stehenden Dienste in der Thin Client-Konfiguration abgeschaltet werden, bzw. die Anmeldung über IGEL Shared Workplace bleibt deaktiviert.

- Nicht zwingend erforderlich – für größere Installationen jedoch empfohlen – ist der Einsatz der **High Availability-Erweiterung** für die IGEL Universal Management Suite. Damit wird eine hohe Verfügbarkeit der Benutzerprofile im Netzwerk gewährleistet.

> Sollten Sie IGEL Shared Workplace mit IGEL Universal Desktop ES verwenden, so achten Sie darauf, dass für den Standardbenutzer **user** kein anderes als das Defaultkennwort **user** gesetzt ist, eine Anmeldung ist sonst nicht möglich.

Konfiguration in der UMS-Konsole

In diesem Kapitel erfahren sie, wie sie

- *ein Active Directory anbinden* (Seite 73),
- *Benutzerprofile zuweisen* (Seite 74),
- *den* Igel Shared Workplace *aktivieren* (Seite 74),
- *den Benutzer-Log-In/out einrichten* (Seite 75) und
- *Prioritäten zuweisen* (Seite 75).

Active Directory anbinden

So binden Sie in der UMS ein Active Directory ein:

1. Klicken Sie **Active Directory** im Bereich **UMS Administration**.
2. Klicken Sie **Hinzufügen**.

   Die Maske **Active Directory / LDAP-Service hinzufügen** öffnet sich.
3. Geben Sie **Domänenname, -controller** und die Zugangsdaten ein.
4. Bestätigen Sie mit **OK**.

   Ihr Active Directory wird nun in der Liste aufgeführt.

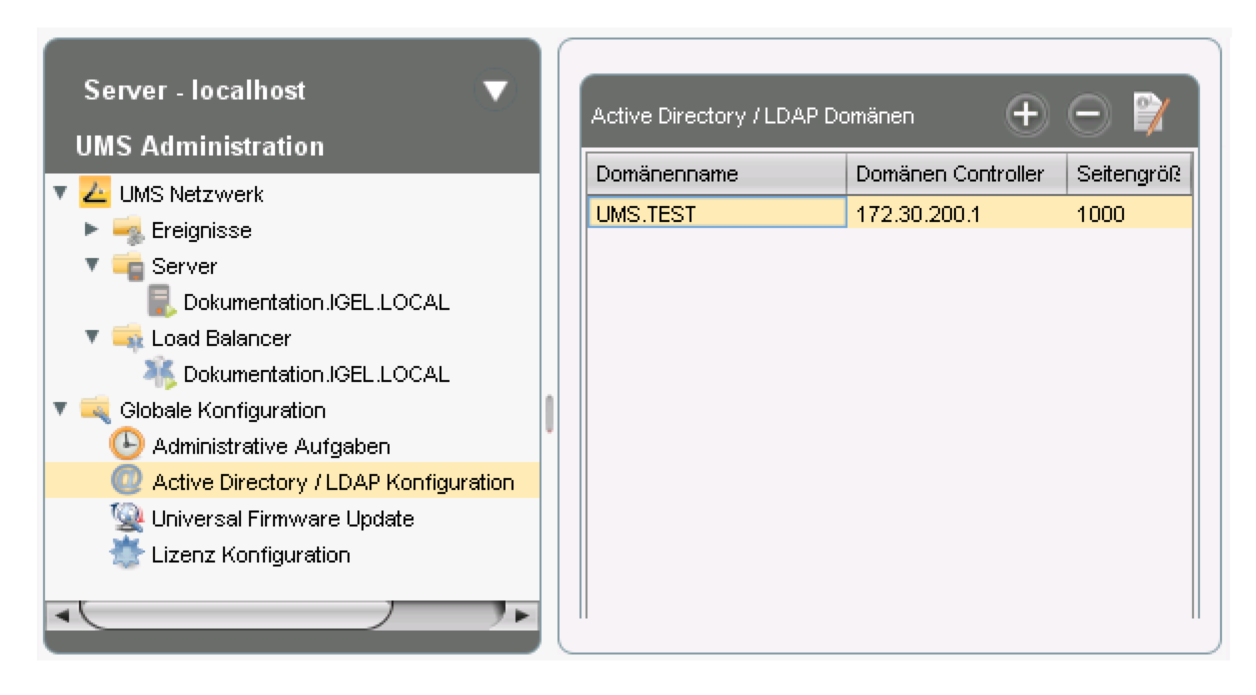


Abbildung 33: Active Directory anbinden

Andere LDAP-Server (Novell eDirectory, OpenLDAP etc.) können nicht für die Benutzerauthentifizierung des IGEL Shared Workplace verwendet werden.

Benutzerprofil zuweisen

- Wechseln Sie in Ihr soeben eingerichtetes Active Directory im UMS Navigationsbaum unter **Server→Shared Workplace Benutzer**.

  Sie können danach browsen oder über Suchen danach suchen.

- Wählen Sie ein Objekt innerhalb der AD-Struktur aus.

  Falls Sie bei der Konfiguration keine Benutzerdaten hinterlegt haben, müssen Sie sich gegenüber dem Active Directory authentifizieren.

- Klicken Sie **Server→Shared Workplace Benutzer→[Active Directory]→[Objekt]**, um diesem Objekt das gewünschte Benutzerprofil zuzuweisen:

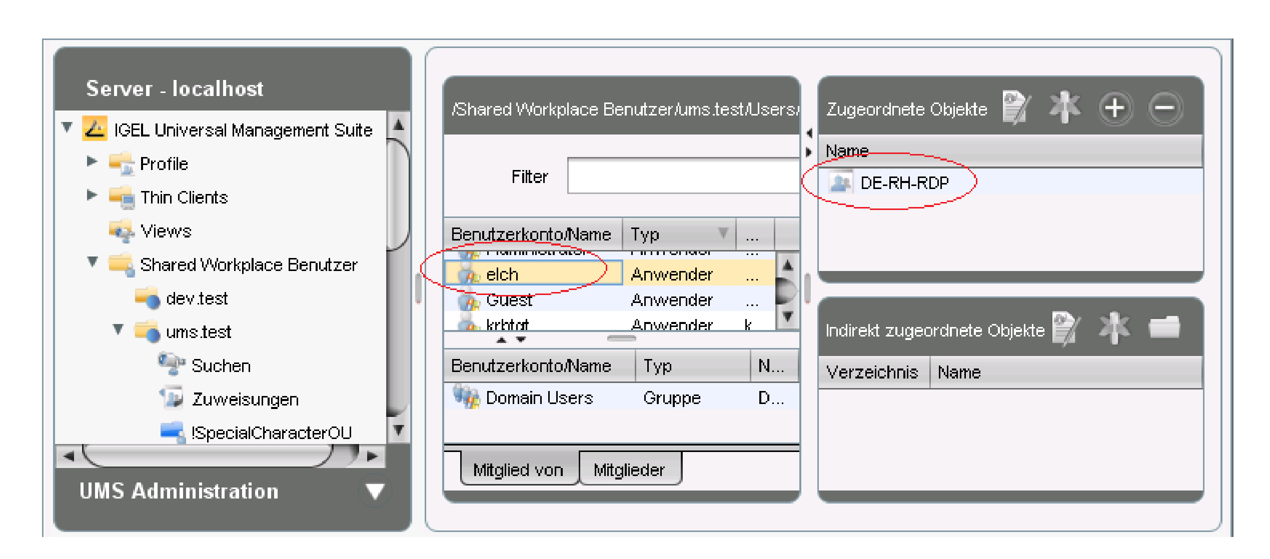


Abbildung 34: Benutzerprofil zuweisen

Es können wie bei Thin Clients auch mehrere Einzelprofile zugewiesen werden. Neben der direkten Zuweisung werden auch indirekt zugewiesene Profile berücksichtigt.

IGEL Shared Workplace am Thin Client aktivieren

Die Einstellungen für Shared Workplace können sie von der UMS aus über ein Profil vornehmen, oder direkt im Setup des jeweiligen Thin Clients.

1. Gehen Sie auf **Konfiguration→Sicherheit→Anmeldung→IGEL Shared Workplace**.
2. Aktivieren Sie die Funktion **IGEL Shared Workplace**.
3. Definieren Sie die **Verknüpfung zum Abmelden** vom System (Linux).

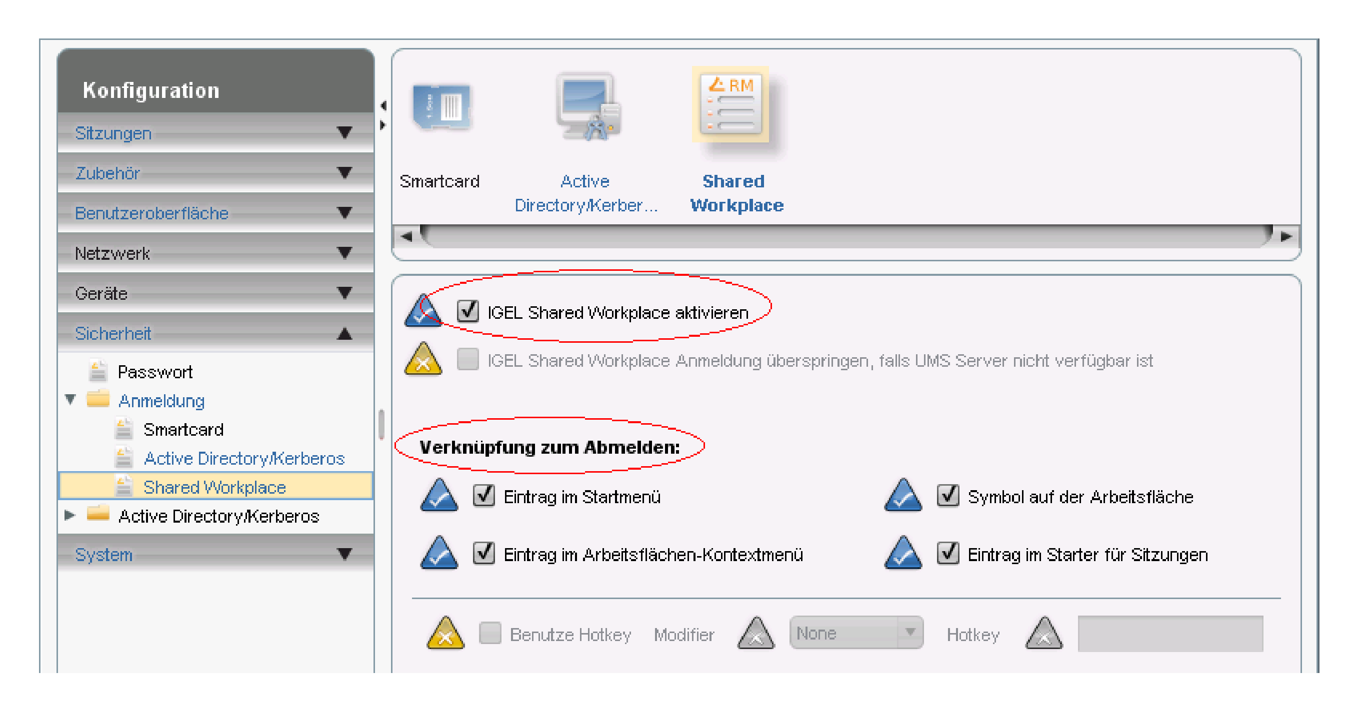


Abbildung 35: IGEL SHARED WORKPLACE aktivieren

Log-in des Benutzers

Um einen Thin Client mit IGEL Shared Workplace starten zu können, benötigt dieser eine Lizenz.

1. Starten Sie den Thin Client.

   Ein Anmeldefenster erscheint.

2. Loggen Sie sich mit Ihren AD-Anmeldedaten ein.

   Sie erhalten die für Sie hinterlegten Profileinstellungen aus der UMS.

Die tatsächlich aktive Konfiguration des Thin Clients für den angemeldeten Benutzer ergibt sich aus der Kumulation aller Profile, die dem Thin Client oder dem Benutzer direkt oder indirekt zugewiesen wurden.

Rangfolge der Profile

Wenn Sie mehrere Profile vergeben, kann es sein, dass bestimmte Benutzer- oder Clienteinstellungen mehrmals belegt sind. Dafür muss eine gewisse Rangordnung festgelegt werden.

Die Priorisierung der Profile ist demnach folgendermaßen definiert:

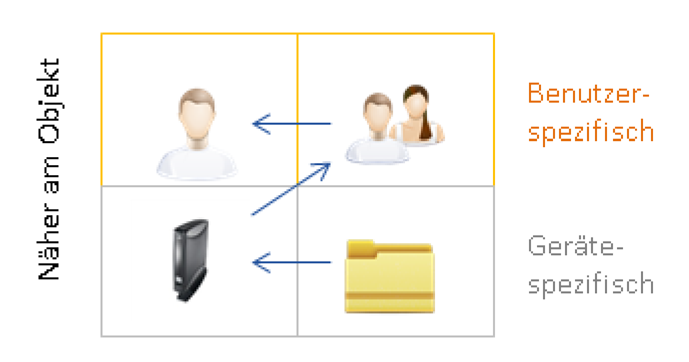


Abbildung 36: Hierarchie der Standardprofile

Höhere Priorität	als...
benutzerspezifische Profile	gerätespezifische Profile
näher am Benutzer/Thin Client	weiter weg vom Benutzer/Thin Client

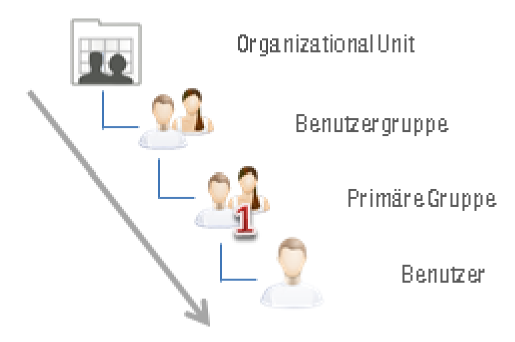


Abbildung 37: Die Priorität der Standardprofile nimmt mit jeder Ebene zu

Höhere Priorität	als...
Primäre Gruppen	sonstige Gruppen
sonstige Gruppen	Organizational Unit

Regeln innerhalb gleicher Ebenen

- Profile, die der primären Gruppe des Benutzers zugewiesen sind, werden in absteigender Reihenfolge nach der Profil-ID priorisiert (höchste ID=höchste Priorität).
- Gruppen innerhalb einer Ebene werden in alphabetischer Reihenfolge priorisiert.
- Direkt dem Benutzer/Gerät zugewiesene Profile werden in absteigender Reihenfolge nach der Profil-ID priorisiert.

Log-out und Benutzerwechsel

Windows Embedded Standard

➢ Melden Sie sich über das Startmenü ab.

IGEL Universal Desktop Linux

Für den Abmeldemodus unter Linux haben Sie folgende Möglichkeiten:

➢ Definieren Sie im **Starter für Sitzungen**, wo Sie die Schaltflächen zum Abmelden ablegen: auf dem Desktop oder im IGEL-Menü.

➢ Definieren Sie im Setup unter **Konfiguration→Sicherheit→Anmeldung→IGEL Shared Workplace** einen Hotkey für die Abmeldung.

6.4.2. Im Benutzerprofil konfigurierbare Parameter

Nicht alle in der jeweiligen Firmware verfügbaren Parameter lassen sich benutzerspezifisch konfigurieren. Dies hat zum Teil technische Gründe und zum Teil liegt es daran, dass einige Parameter nur für die Gerätekonfiguration, nicht aber für die Benutzerkonfiguration sinnvoll sind.

Die **nicht wirksam** konfigurierbaren gerätespezifischen Systemeinstellungen der IGEL-Betriebssysteme sind im folgenden aufgelistet. Es findet keine Prüfung in der IGEL UMS statt.

Universal Desktop Linux (Seite 77)

Universal Desktop Windows Embedded Standard (Seite 78)

Gerätespezifische Parameter UD Linux

Im Benutzerprofil sind folgende Systemeinstellungen **nicht** konfigurierbar:

- Netzwerkeinstellungen inkl. der Netzlaufwerke
- Bildschirmkonfiguration bei IGEL Linux v5 bis 5.05.100 und bei IGEL Linux v4 bis 4.13.100.

> Auch unter IGEL Linux ab Release 4.14.100 und 5.06.100 kann es abhängig von der verwendeten Hardware nach Änderung der Auflösung oder Rotation durch den Benutzer zu Darstellungsfehlern kommen. Hinweise zum Einrichten der Bildschirmkonfiguration für IGEL Shared Workplace gibt ein Best-Practice-Dokument.

- Touchscreenkonfiguration
- Updateeinstellungen
- Sicherheitseinstellungen
- Remote Management
- Kundenspezifische Partition
- Server für Hintergrundbilder
- Kundenspezifischer Bootbildschirm
- Browser-Plug-ins
- SCIM-Eingabemethoden, die Aktivierung ist aber benutzerspezifisch möglich
- Emulation 3-Tasten-Maus
- Appliance Mode (VMware View, Citrix XenDesktop und Spice)

Gerätespezifische Einstellungen UD W7

Diese Systemeinstellungen sind **nicht** im Benutzerprofil konfigurierbar:

- Sprache, Standards und Formate
- Netzwerkeinstellungen inkl. der Netzlaufwerke
- Active Directory-Anmeldung
- USB-Gerätekonfiguration
- Liste der verfügbaren Features und Windows Services
- Updateeinstellungen
- Setupsitzung
- Benutzer- und Sicherheitseinstellungen
- Dateibasierender Schreibfilter
- Energieoptionen
- Remote Management
- Appliance Mode (VMware View und Citrix XenDesktop)

6.5. Masterprofile

Ziel der Einführung von Masterprofilen ist es, die komplexere Rechteverwaltung für UMS-Administratoren in sehr großen oder verteilten Umgebungen abbilden zu können. Wichtige Profilkonfigurationen können nun allen registrierten Thin Clients priorisiert zugewiesen werden, ohne gleichzeitig anderen Administratoren Verwaltungsrechte für andere Einstellungen oder Profile entziehen zu müssen.

Masterprofile werden in einem eigenen Abschnitt im Navigationsbaum der IGEL UMS aufgeführt. Sie sind von ihrer Wirkungsweise her mit den Standardprofilen identisch, werden jedoch anders priorisiert. Masterprofile sind Profile, deren Einstellungen alle Standardprofile übersteuern.

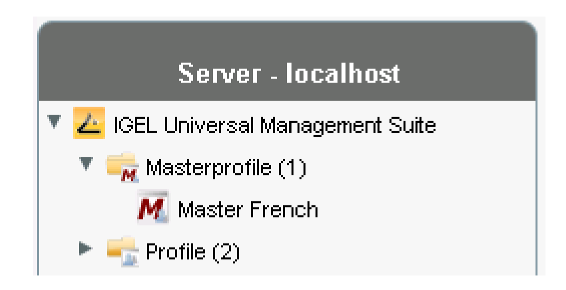


Abbildung 38: Masterprofile im Baum

6.5.1. Masterprofile aktivieren

Sie können selber bestimmen, ob Sie Masterprofilen einsetzen möchten oder nicht. Standardmäßig sind sie aktiviert.

So deaktivieren Sie die Funktion **Masterprofile**:

1. Gehen Sie in der **UMS Administration** unter **Zusätzliche Einstellungen**.
2. Deaktivieren Sie **Masterprofile**.

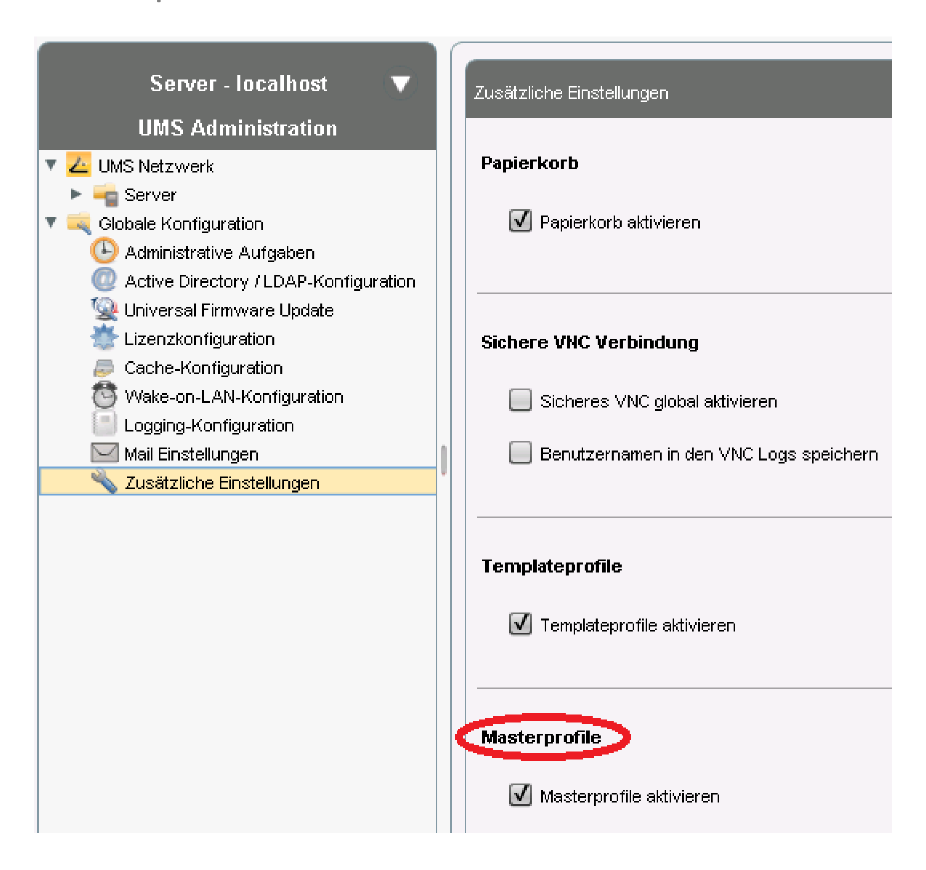


Abbildung 39: Masterprofile deaktivieren

6.5.2. Rangfolge der Profile

Masterprofile übersteuern alle Standardprofile.

Masterprofile sind hinsichtlich ihrer Priorisierung untereinander umgekehrt gestaffelt als die Standardprofile. Das heißt, eine konkurrierende Profileinstellung ist umso höher priorisiert, je weiter oben in der Hierarchie das Profil zugeordnet ist, d.h. je weiter es vom Objekt entfernt ist.

Die Priorisierung der Masterprofile ist demnach folgendermaßen definiert:

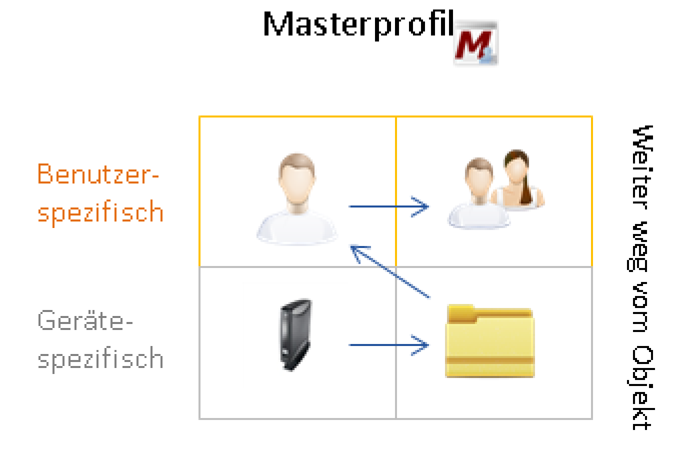


Abbildung 40: Hierarchie der Masterprofile

Höhere Priorität	als...
benutzerspezifische Profile	gerätespezifische Profile
weiter weg vom Benutzer/Thin Client	näher am Benutzer/Thin Client

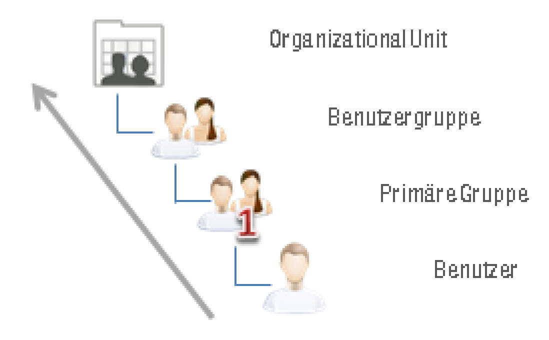


Abbildung 41: Die Priorität der Masterprofile nimmt mit jeder Ebene ab

Höhere Priorität	als...
Organizational Unit	sonstige Gruppen
sonstige Gruppen	Primäre Gruppe

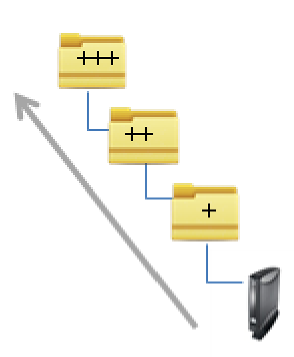


Abbildung 42: Die Priorität der Masterprofile nimmt mit jeder Ebene ab

Höhere Priorität	als...
weiter weg vom Thin Client	näher am Thin Client
übergeordnetes Verzeichnis	Unterverzeichnis

Kurzform der Priorisierung insgesamt in absteigender Reihenfolge

1. Benutzerspezifische Masterprofile ("näher" am Benutzer bedeutet geringere Priorität)
2. Gerätespezifische Masterprofile ("näher" am Gerät bedeutet geringere Priorität)
3. Benutzerspezifische Standardprofile ("näher" am Benutzer bedeutet höhere Priorität)

4. Gerätespezifische Standardprofile ("näher" am Gerät bedeutet höhere Priorität)

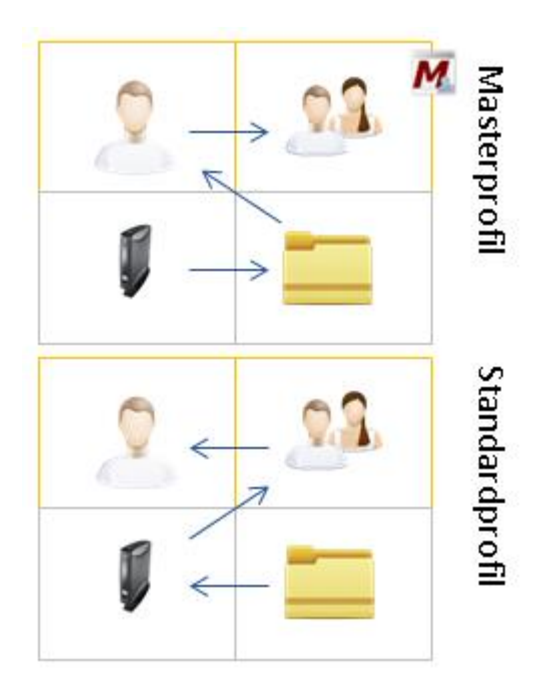


Abbildung 43: Kurzform der Priorisierung

Regeln innerhalb gleicher Ebenen

- Masterprofile, die der primären Gruppe des Benutzers zugewiesen sind, werden in absteigender Reihenfolge nach der Profil-ID priorisiert.
- Gruppen innerhalb einer Ebene werden in alphabetischer Reihenfolge priorisiert.
- Direkt dem Benutzer/Gerät zugewiesene Masterprofile werden in absteigender Reihenfolge nach der Profil-ID priorisiert.

6.6. Templateprofile

Ein **Templateprofil** erlaubt es, einzelne Parameter im Profil mit Variablen zu belegen und deren **Werte** Thin Clients zuzuweisen.

Standardprofile UND Masterprofile können durch den Einsatz von Variablen zu Templateprofilen werden.

Anwendungsbeispiel

Die Thin Clients eines Unternehmens sind auf mehrere Niederlassungen verteilt. Alle Clients sollen über ein Profil eine Browsersitzung mit gleichen Einstellungen erhalten, allerdings soll in den globalen Einstellungen für jede Niederlassung eine andere Startseite konfiguriert werden, außerdem soll der Sitzungsname für jede Niederlassung individuell gesetzt werden.

Bisherige Lösung

Bisher legt man für jede Niederlassung ein eigenes Profil mit globalen Einstellungen und Sitzungsdaten an. Manchmal lässt sich die gewünschte Kombination von Einstellungen auch über Vererbung verschiedener Profile erreichen.

Problem

Oft lassen sich die gewünschten Einstellungen über verschiedene Profile aber nicht kombinieren, z. B. für die Konfiguration einer Sitzung. Außerdem ist die unnötige Vielzahl an Profilen auf Dauer schwer zu verwalten.

Lösung

Flexibler ist der Einsatz eines einzigen Templateprofils. Dieses enthält alle Daten für die Browsersitzung, die den Thin Clients gemeinsamen sind und zusätzlich Platzhalter, sogenannte **Templateschlüssel**. Die Templateschlüssel enthalten Parameter, die für unterschiedliche Clients an unterschiedlichen Standorten abweichende Werte erhalten sollen.

Das Templateprofil wird dann direkt oder indirekt den Clients zugewiesen. Die standortbezogenen Templatewerte werden jeweils den Clients zugewiesen, die diesen Templatewert erhalten sollen.

Der Thin Client erhält damit ein Profil, dessen Einstellungen sich aus den fest im Profil gepflegten Daten und den ihm zugewiesenen Templatewerten zusammensetzt, die durch Templateschlüssel im Profil referenziert werden.

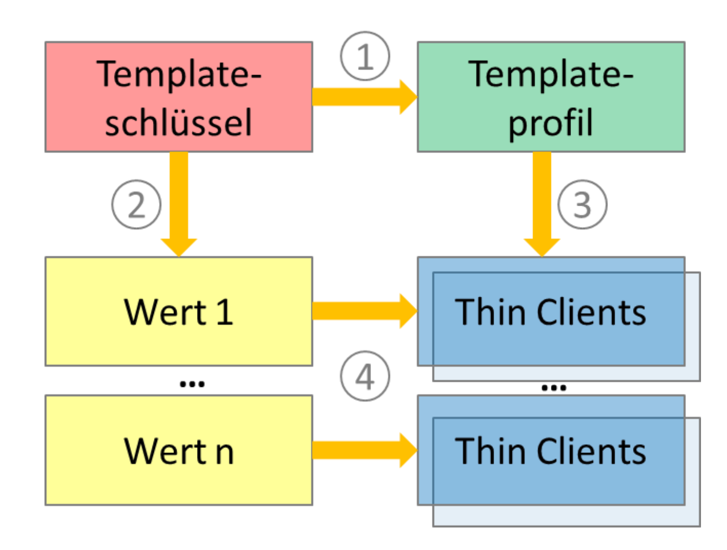


Abbildung 44: Funktionsschema Templateprofile

1. Templateschlüssel werden in einem oder mehreren Profilen verwendet.
2. Ein Templateschlüssel hat mehrere Werte.
3. Das Templateprofil wird mehreren Thin Clients direkt oder indirekt zugewiesen.
4. Ein Wert des Schlüssels kann jeweils einem oder mehreren Thin Clients zugewiesen werden.

Ein Thin Client erhält somit neben den allgemeinen Einstellungen des Profils auch den ihm zugewiesenen Templatewert an der Stelle der Konfiguration, die im Profil durch den zugehörigen Templateschlüssel als Platzhalter repräsentiert ist.

6.6.1. Templateprofile aktivieren

Wenn Sie die Funktion Templateprofile nutzen möchten, müssen Sie diese erst aktivieren.

➢ Aktivieren Sie Templateprofile in der UMS Konsole unter UMS Administration→Globale Konfiguration→Zusätzliche Einstellungen.

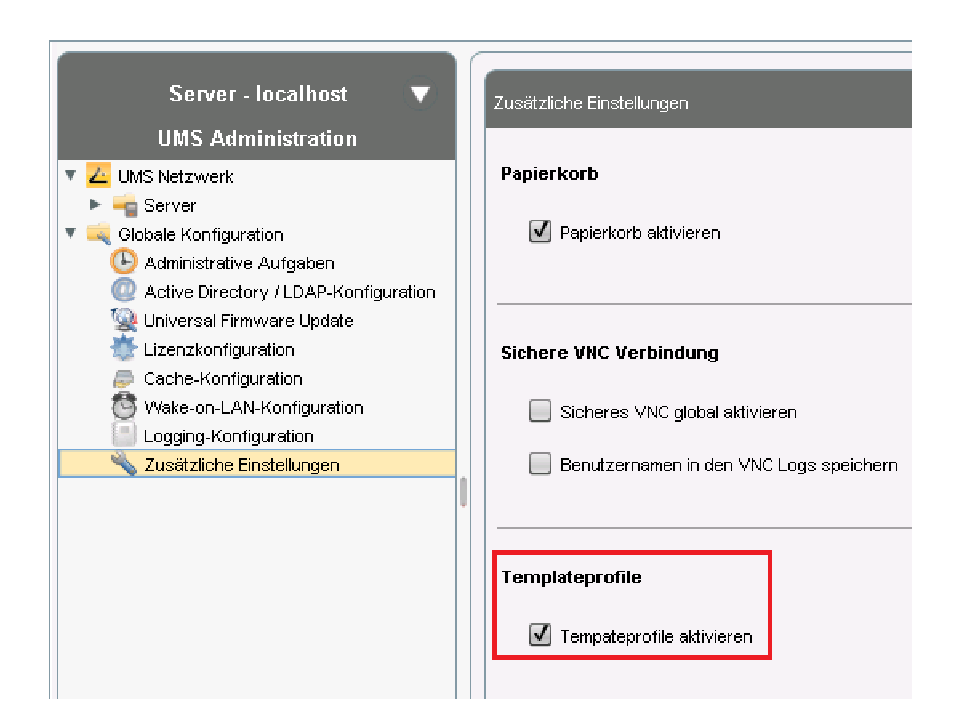


Abbildung 45: Templateprofile aktivieren

Im Navigationsbaum öffnet sich der Knoten Templateschlüssel und Wertesammlungen:

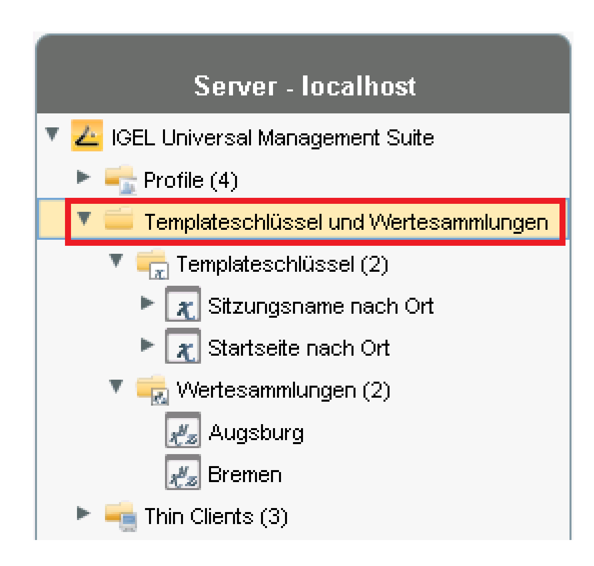


Abbildung 46: Templateschlüssel und Wertesammlungen

6.6.2. Templateschlüssel und Werte erstellen

So erstellen Sie Templateschlüssel und Werte:

1. Öffnen Sie das Kontextmenü des Ordners **Templateschlüssel**.
2. Klicken Sie **Neuer Templateschlüssel**.

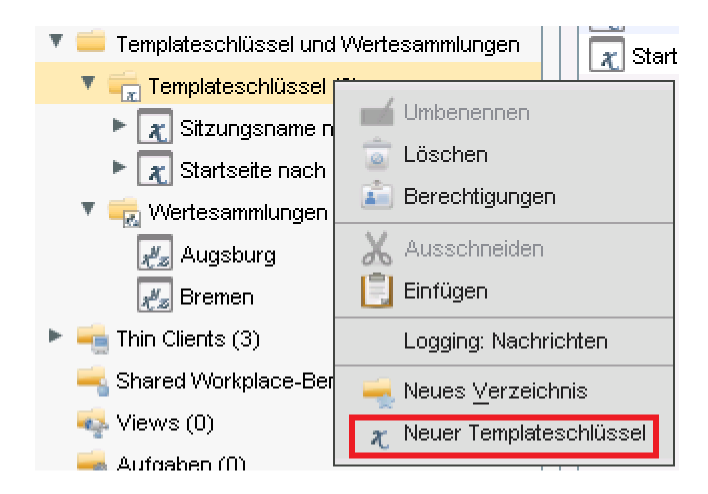


Abbildung 47: Neuen Templateschlüssel anlegen

> Alternativ ist diese Funktion auch erreichbar über das Menü **System→Neu→Neuer Templateschlüssel**, dazu muss der Fokus auf dem Knoten **Templateschlüssel** liegen.

Ein Assistent führt Sie durch die Schritte der Neuanlage:

3. Definieren Sie einen **Namen** für den Schlüssel.
4. Wählen Sie einen **Werttyp** für den Schlüssel (Zeichenkette, Wahrheitswert, Ganz- oder Gleitkommazahl).
5. Erfassen Sie optional eine **Beschreibung** des Schlüssels.
6. Klicken Sie **Weiter**.

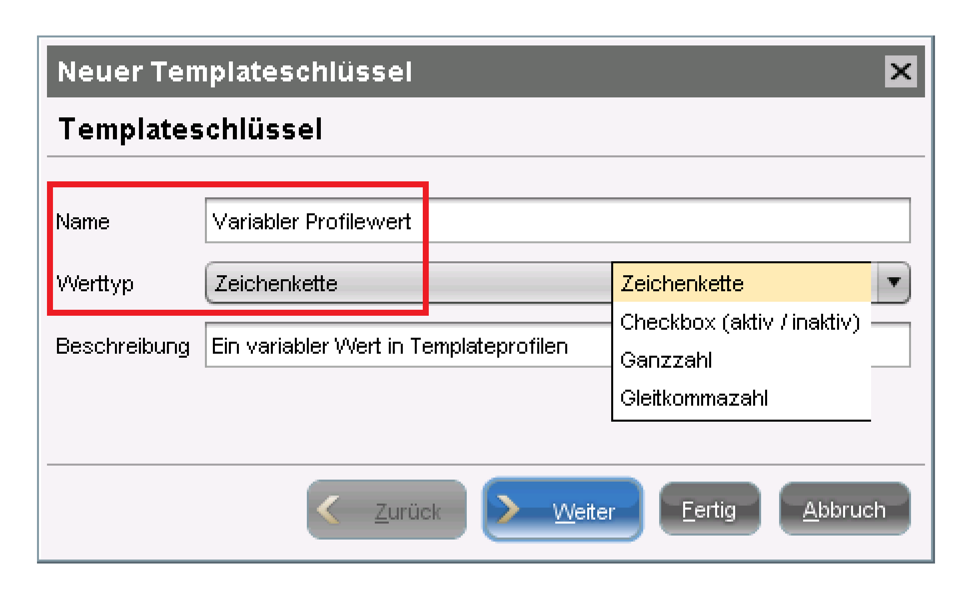


Abbildung 48: Basisdaten eines Templateschlüssels

So legen Sie den ersten Wert des Schlüssels an:

1. Erfassen Sie den gewünschten Parameterwert im Feld **Wert**.
2. Ergänzen Sie optional eine **Beschreibung** des Werts.
3. Klicken Sie **Wert anlegen**.

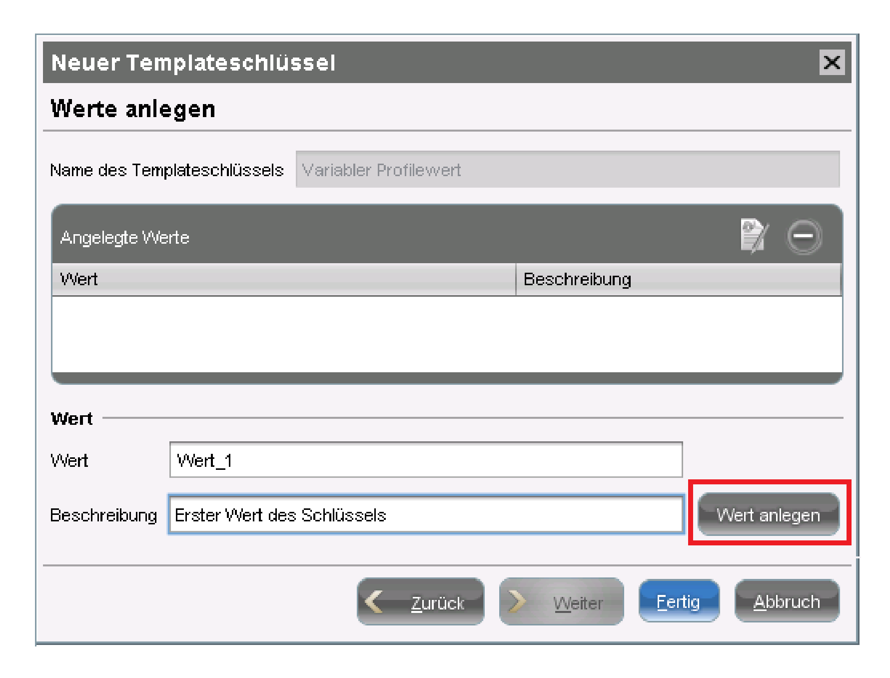


Abbildung 49: Wert zum Schlüssel anlegen

So legen Sie weitere Werte des Schlüssels an:

1. Ändern Sie die Eintragungen unter **Wert** und **Beschreibung**.

2. Klicken Sie erneut **Wert anlegen**.
3. Klicken Sie **Fertig**, um den Schlüssel mit seinen Werten zu speichern, nachdem Sie alle gewünschten Werte angelegt haben.

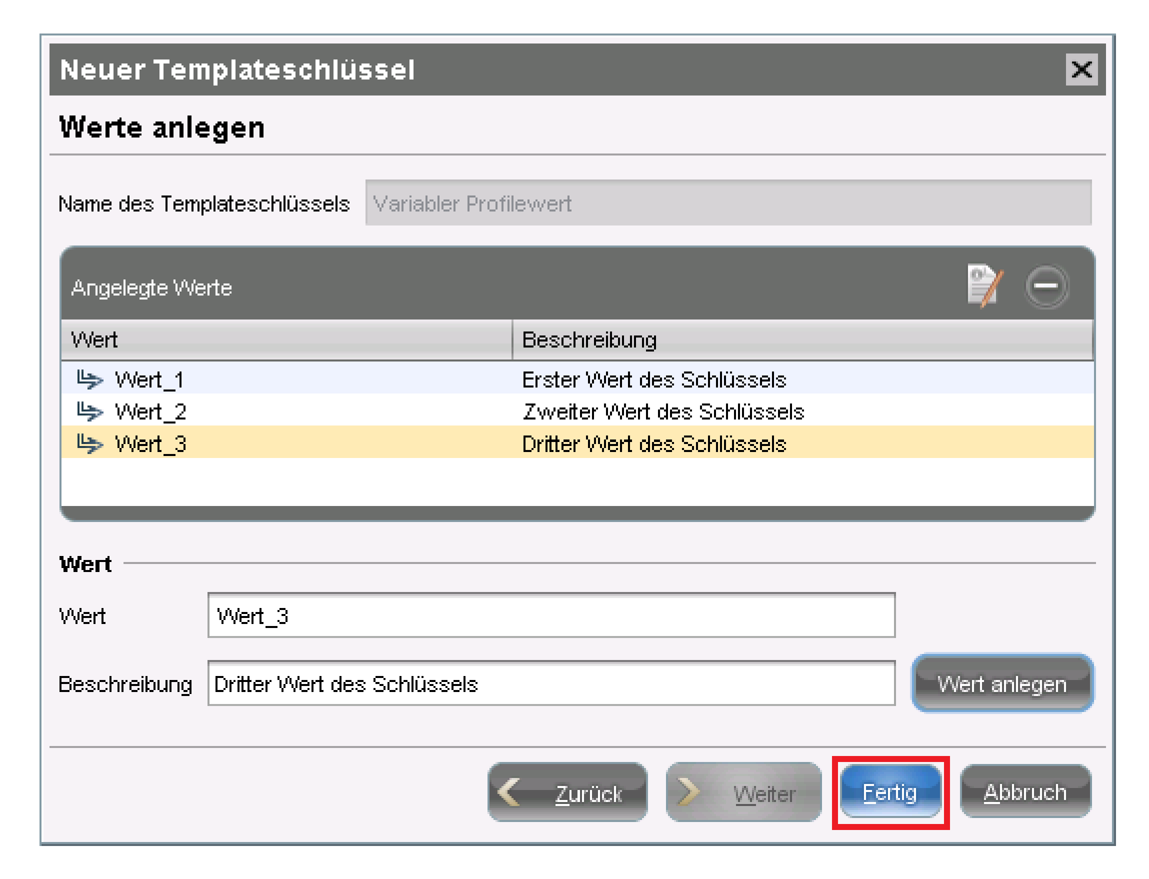


Abbildung 50: Neue Templateschlüssel

Der Schlüssel wird mit seinen Werten im Baum angezeigt:

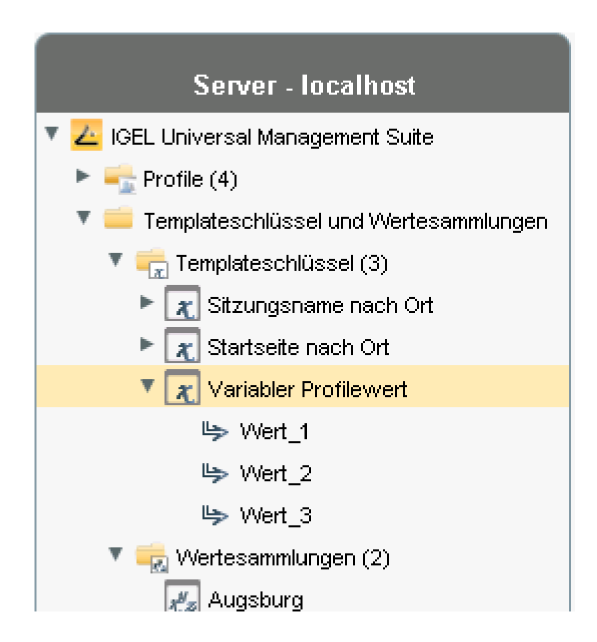


Abbildung 51: Templateschlüssel und seine Werte

Als Workflow empfehlen wir, die Templateschlüssel und Werte aus der *Profilkonfiguration* (Seite 89) heraus anzulegen.

Schlüssel und Werte im Profil erstellen

In Profilen lassen sich bestimmte Parameter mit Templateschlüssel konfigurieren. Damit verbinden Sie folgende Schritte zu einem Workflow:

- *Templateschlüssel und Werte erstellen* (Seite 86)
- *Templateschlüssel in Profilen verwenden* (Seite 91)

So nutzen Sie Templateschlüssel bei der Konfiguration eines Profils:

1. Öffnen Sie ein bestehendes **Profil** oder legen Sie ein neues Profil an.
2. Klicken Sie **Konfiguration bearbeiten**, um die zu pflegenden Parameter aufzurufen.
3. Konfigurieren Sie wie gewohnt diejenigen **Parameterwerte**, die für alle Thin Clients mit diesem Profil gelten sollen.
4. Wählen Sie einen Parameter, der einen clientspezifischen Wert aus einem **Templateschlüssel** beziehen soll.
5. Klicken Sie das Aktivierungssymbol vor dem Parameter, bis die gewünschte Funktion aktiv ist (hier:Templateschlüssel aktiv):

 Der Parameter ist inaktiv und wird nicht durch das Profil konfiguriert.

 Der Parameter ist aktiv und der eingestellte Wert wird durch das Profil konfiguriert, Templateschlüssel sind für den Parameter nicht verfügbar.

 Der Parameter ist aktiv und der eingestellte Wert wird durch das Profil konfiguriert, Templateschlüssel sind für den Parameter verfügbar.

 Templateschlüssel sind aktiv für diesen Parameter, das Profil erhält hier später einen Wert des Schlüssels.

Manche Parameter können nicht mit Templateschlüsseln konfiguriert werden und bieten nur die Optionen inaktiv und aktiv. Dies gilt z.B. für Kennwörter oder Parameter, die von anderen Konfigurationseinstellungen abhängig sind.

6. Klicken Sie das **Auswahlsymbol** , um einen Templateschlüssel zu wählen.
7. Klicken Sie **Hinzufügen** , um einen neuen Templateschlüssel anzulegen.

   Ein Assistent führt Sie durch die Schritte der Neuanlage:
8. Geben Sie einen **Namen** für den Schlüssel an.

Der **Werttyp** für den Schlüssel ist durch den Parameter vorgegeben.

9. Geben Sie optional eine **Beschreibung** des Schlüssels an.



Abbildung 52: Anlegen eines Templateschlüssels

10. Klicken Sie **Weiter**.

So erfassen Sie den ersten Wert des Schlüssels:

1. Definieren Sie den gewünschten Parameterwert im Feld **Wert**.
2. Ergänzen Sie optional eine **Beschreibung** des Werts.
3. Klicken Sie **Wert anlegen**.

> Bei Parametern mit festem Wertebereich, wie Auswahlmenü oder Checkbox, werden die vorhandenen Optionen zur Wahl gestellt. Klicken Sie **Alle anlegen**, um Werte für jeden Eintrag des Wertebereichs zu erstellen oder fügen Sie mit **Wert anlegen** nur ausgewählte Einträge hinzu.

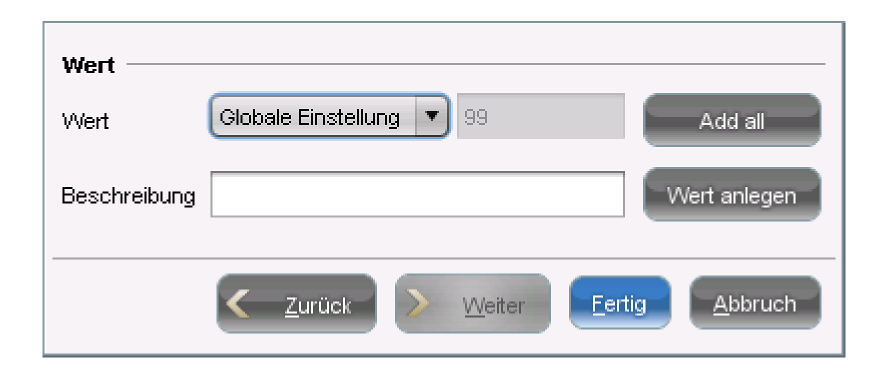


Abbildung 53: Definieren einses Wertes für den Templateschlüssel

4. Klicken Sie **Fertig**, um den Schlüssel mit seinen Werten zu speichern.
5. Klicken Sie **OK**, um in das Profil zurück zu gelangen.

   Der Schlüssel wird im Profilparameter angezeigt:

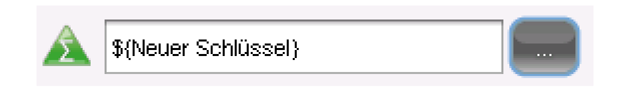


Abbildung 54: Neuer Templateschlüssel

6. **Speichern** Sie das Templateprofil.

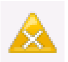
   Profile, die mindestens einen Templateschlüssel in der Konfiguration verwenden, werden im Navigationsbaum durch ein spezielles Symbol gekennzeichnet: .

6.6.3. Templateschlüssel in Profilen verwenden

Templateschlüssel werden im Navigationsbaum im Knoten **Templateschlüssel und Wertesammlungen / Templateschlüssel** aufgelistet. Sie lassen sich in eigene Unterordner verschieben.

So verwenden Sie einen Templateschlüssel im Profil:

1. Öffnen Sie ein bestehendes **Profil** oder legen Sie ein neues Profil an.
2. Rufen Sie in der Profilkonfiguration die zu pflegenden Parameter auf.
3. Konfigurieren Sie wie gewohnt diejenigen Parameterwerte, die allen Thin Clients mit diesem Profil gemeinsam sein sollen.
4. Wählen Sie nun einen Parameter, der mit clientspezifischen Werten aus einem **Templateschlüssel** versorgt werden soll.
5. Klicken Sie das **Aktivierungssymbol** vor dem Parameter, bis die gewünschte Funktion aktiv ist (hier:Templateschlüssel aktiv):

 Der Parameter ist inaktiv und wird nicht durch das Profil konfiguriert.

 Der Parameter ist aktiv und der eingestellte Wert wird durch das Profil konfiguriert, Templateschlüssel sind für den Parameter nicht verfügbar.

 Der Parameter ist aktiv und der eingestellte Wert wird durch das Profil konfiguriert, Templateschlüssel sind für den Parameter verfügbar.

 Templateschlüssel sind aktiv für diesen Parameter, das Profil erhält hier später einen Wert des Schlüssels.

> Manche Parameter können nicht mit Templateschlüsseln konfiguriert werden und bieten nur die Optionen inaktiv und aktiv. Dies gilt z.B. für Kennwörter oder Parameter, die von anderen Konfigurationseinstellungen abhängig sind.

6. Klicken Sie das Auswahlsymbol , um einen Templateschlüssel zu wählen.
7. Doppelklicken Sie den gewünschten **Templateschlüssel**.

> Oder legen Sie einen neuen Schlüssel an, siehe *Schlüssel und Werte im Profil erstellen* (Seite 89).

8. Klicken Sie **OK**.
9. **Speichern** Sie das Templateprofil.

   Profile, die mindestens einen Templateschlüssel in der Konfiguration verwenden, werden im Navigationsbaum durch ein spezielles Symbol gekennzeichnet: .

6.6.4. Templateprofile und Werte den Thin Clients zuordnen

Nachdem Sie die **Templateschlüssel** und **Werte** und die Konfiguration von **Profilen** unter Verwendung der Templateschlüssel angelegt haben, müssen Sie die Schlüssel und Werte am Thin Client wieder zusammenführen.

So weisen Sie einem Thin Client ein Templateprofil und die für die Ersetzung der Schlüssel notwendigen Werte zu:

1. Wählen Sie ein **Templateprofil** und ordnen Sie es wie üblich einer Gruppe von Thin Clients oder einem Thin Client-Verzeichnis zu.
2. Wählen Sie zu jedem im Profil verwendeten **Templateschlüssel** einen **Wert** aus.
3. Ordnen Sie die jeweiligen Werte den entsprechenden Thin Clients zu.

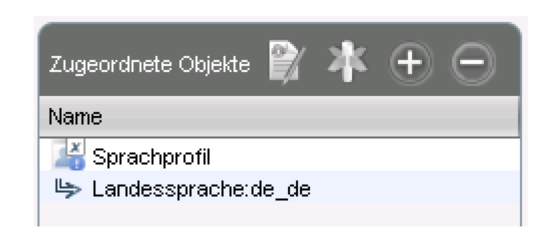


Abbildung 55: Beispiel Templateprofil und Wertzuordnung

4. Ordnen Sie weitere Werte der Schlüssel weiteren Thin Clients zu. Es lassen sich auch mehrere Werte verschiedener Schlüssel gesammelt zuordnen (Tasten Umschalt und Strg).

> Jeder Thin Client muss anschließend für jeden Schlüssel in den zugewiesenen Profilen auch einen zugewiesenen Wert besitzen.

So prüfen Sie die richtige Zuordnung von Templateprofilen und Werten:

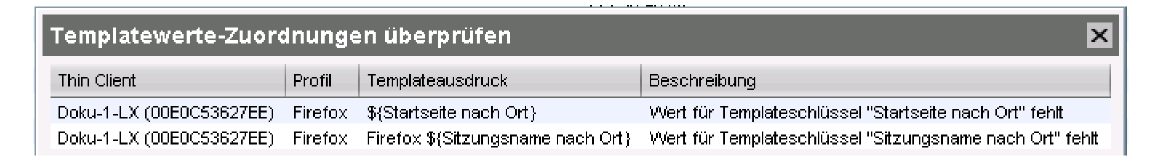
1. Klicken Sie in der oberen Menüleiste **Thin Clients**.
2. Wählen sie **Templatewerte-Zuordnungen überprüfen**.

   Die ausgewählten und geprüften Thin Clients werden dem Ergebnis entsprechend gekennzeichnet:

    alle Templateschlüssel sind definiert

    fehlende Templateschlüssel

3. Doppelklicken Sie auf die Meldung im Nachrichtenfenster, um das Fehlerprotokoll der Prüfung zu öffnen:



Templatewerte-Zuordnungen überprüfen

Thin Client	Profil	Templateausdruck	Beschreibung
Doku-1-LX (00E0C53627EE)	Firefox	${Startseite nach Ort}	Wert für Templateschlüssel "Startseite nach Ort" fehlt
Doku-1-LX (00E0C53627EE)	Firefox	Firefox ${Sitzungsname nach Ort}	Wert für Templateschlüssel "Sitzungsname nach Ort" fehlt

Abbildung 56: Prüfungsprotokoll

Oder klicken Sie einen Thin Client, auch hier werden die Prüfergebnisse direkt angezeigt:

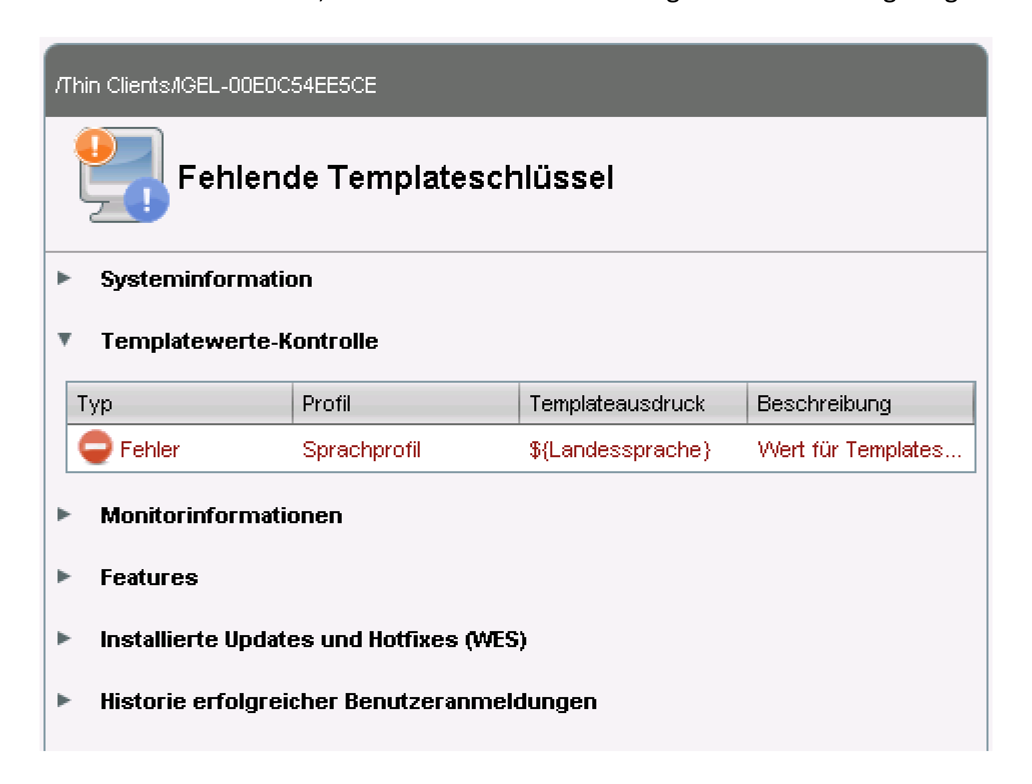


Abbildung 57: Prüfergebnisse am Thin Client

Sobald die Thin Clients ihre aktualisierten Profileinstellungen erhalten (z.B. automatisch nach dem Neustart der Clients), werden für jeden Thin Client die im Profil enthaltenen Schlüssel durch den entsprechenden Wert aus deren Zuordnung zum Thin Client ersetzt und an den Thin Client übermittelt. Das lokale Setup des Thin Clients enthält somit nur die üblichen Parameterwerte und keine Schlüssel mehr.

6.6.5. Wertesammlungen

In Wertesammlungen lassen sich logisch zusammengehörige Werte verschiedener Templateschlüssel zusammenfassen und gemeinsam Thin Clients zuordnen.

Haben Sie z.B. verschiedene Profile, die länderspezifische Einstellungen über Templateschlüssel und Wertzuweisungen erhalten sollen, so können alle Werte für ein Land / eine Sprache in einer Wertesammlung gruppiert werden. Ein Thin Client erhält mit Zuordnung einer solchen Sammlung auch alle darin enthaltenen Werte für sein Land / seine Sprache.

So legen Sie eine Wertesammlung an:

1. Legen Sie ein **Templateprofil** mit Schlüsseln und Werten an.
2. Klicken Sie **System→Neu→Neue Wertesammlung**, um eine neue Wertesammlung anzulegen.

3. Tragen Sie **Namen** und **Beschreibung** für die Sammlung ein.

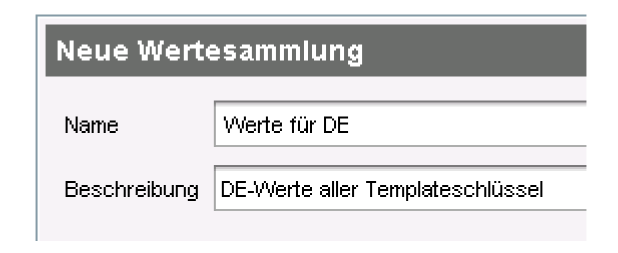


Abbildung 58: Neue Wertesammlung anlegen

4. Wählen Sie aus jedem Schlüssel die gültigen Werte aus, eine Mehrfachauswahl ist möglich.

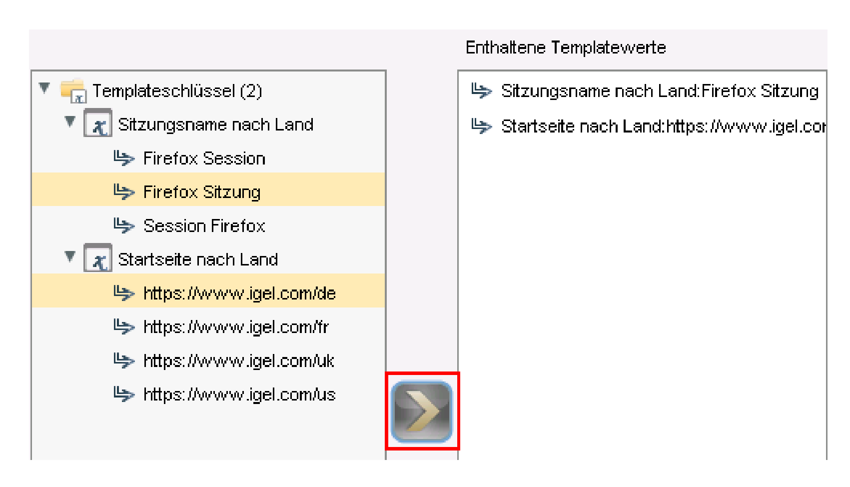


Abbildung 59: Schlüsselwerte auswählen

5. Bestätigen Sie mit **OK**.
6. Legen sie weitere Wertesammlungen an.

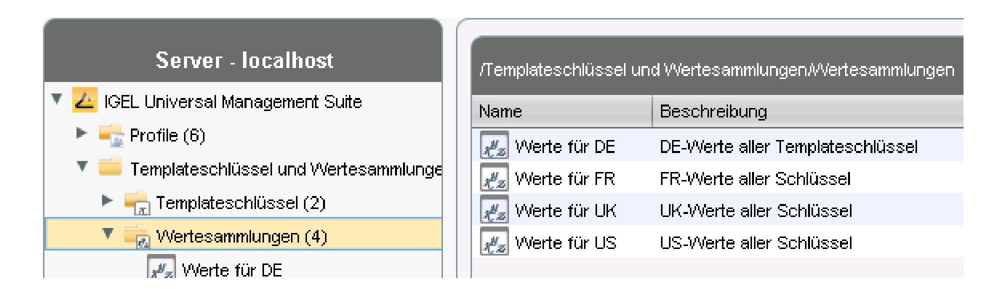


Abbildung 60: Eine Wertesammlung je Land

7. Weisen Sie das Templateprofil allen Thin Clients zu.
8. Weisen Sie den Geräten jeweils die passende Wertesammlung zu.
9. Markieren Sie den Baumknoten **Thin Clients**.
10. Klicken Sie im Menü unter **Thin Clients→Templatewerte-Zuordnungen prüfen**, um die Zuordnungen zu prüfen.

    Das Ergebnis wird Ihnen im Nachrichtenfenster angezeigt.

Die Thin Clients erhalten beim nächsten Neustart oder nach manueller Übermittlung die neuen Sitzungsdaten mit gemeinsamen und länderspezifischen Einstellungen des Profils.

Der Vorteil dieser Methode ist, dass Sie in Zukunft weitere Schlüsselwerte nur noch der entsprechenden Wertesammlung hinzufügen müssen, um diese den Thin Clients der Niederlassung zuzuweisen. Zusätzlich verbessert sich die Übersicht bei großer Zahl an Templateschlüsseln und Werten.

7. Views

Eine Thin Client-View, auch Ansicht genannt, ist eine Auswahl der in der Datenbank verfügbaren Thin Clients, die anhand definierbarer Regeln erstellt wird. Alle Thin Clients, die diese Regel erfüllen, werden in der View angezeigt.

Beispiel:

Sie möchten sich eine Liste der Thin Clients ansehen, die eine IP-Adresse in einem bestimmten Adressbereich haben. Um diese Liste zu generieren, können Sie eine View erstellen, deren Regel durch den IP-Adressbereich bestimmt wird. Die Views werden im Navigationsbaum der UMS angezeigt, und Sie können hierfür Zugriffsrechte konfigurieren.

Views dienen nicht nur der Information über Inhalte der Datenbank, sie lassen sich z. B. auch einsetzen, um geplante Aufgaben, wie ein Firmwareupdate, für eine bestimmte Auswahl von Thin Clients zu definieren. Sie müssen die zu aktualisierenden Thin Clients somit nicht einzeln der Aufgabe zuweisen. Die Geräte werden stattdessen zur Laufzeit der Aufgabe per View ermittelt, etwa anhand der bereits installierten Firmware.

Eine View nimmt keine Änderungen an Thin Client-Einstellungen oder der Verzeichnisstruktur des UMS-Baums vor. Sie bietet lediglich eine spezielle Ansicht der Thin Clients, die in der UMS registriert sind.

7.1. Neue View erstellen

So erstellen Sie eine neue View:

1. Gehen Sie mit der Maus auf den Baumknoten **Views**.
2. Wählen Sie im Kontextmenü **Neue View**

   oder wählen Sie im Menü **System→Neu→Neue View**.
   Das Fenster **Neue View erzeugen** öffnet sich.
3. Vergeben Sie einen Namen und eine nähere Beschreibung der View.
4. Klicken Sie **Weiter**.

   Das Fenster **Suchparameter auswählen** öffnet sich.
5. Verknüpfen Sie nach und nach mehrere Kriterien logisch miteinander.
6. Definieren Sie die Viewparameter, z. B. für die Firmware unter 4.09.100 wenn Sie dieses Update verteilen möchten und alle Clients mit älterer Firmware aktualisiert werden sollen.

   Als Vergleichsoperatoren stehen **Gleich**, **Größer als**, **Kleiner als** zur Verfügung, ebenso die Möglichkeit, einen regulären Ausdruck für die Suche zu definieren.
7. Klicken Sie **Weiter**.

   Das Fenster **Neue View erzeugen** öffnet sich.
8. Klicken Sie **View erzeugen**, um die View fertigzustellen

   oder spezifizieren Sie die Suche weiter.

Im gewählten Beispiel fügen wir noch eine Einschränkung anhand der Produkt-ID hinzu, um die Selektion auf UD LX-Geräte zu beschränken, für welche die neue Firmware geeignet ist. Dazu wählen Sie den regulären Ausdruck `UD.*LX`, um alle Gerätetypen der Universal Desktop Linux-Reihe zu erfassen.

7.1.1. Beispiel View erstellen

Die einzelnen Schritte des Beispiels:

1. Wir geben Namen und Beschreibung der View an: `Update UDLX, Update auf 4.09.100`

   und wählen einen ersten Suchparameter: **Firmwareversion**

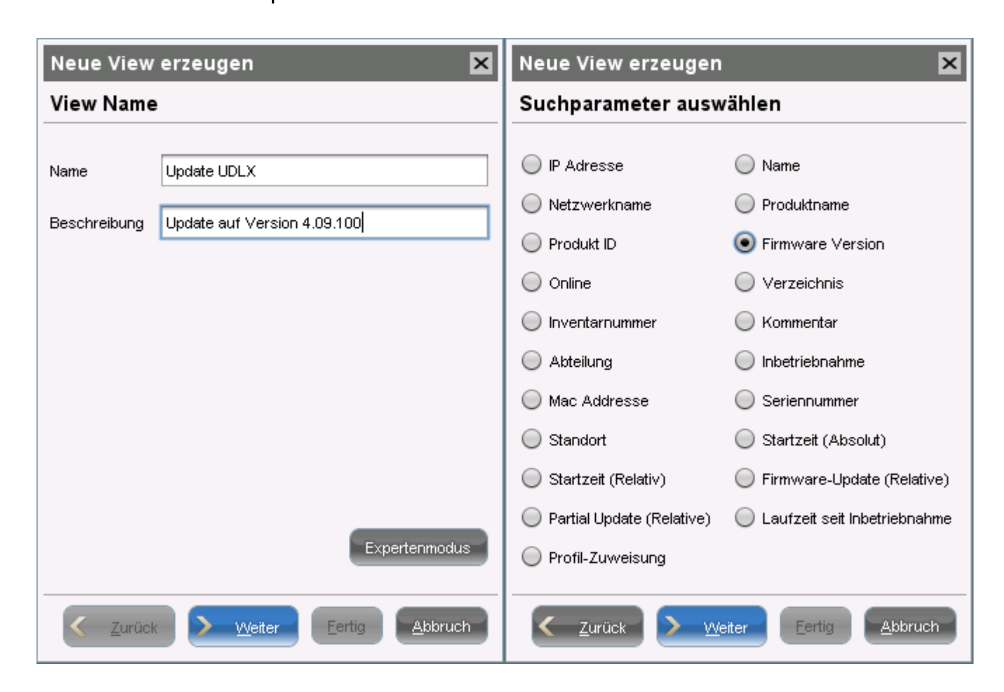


Abbildung 61: Suchparameter erzeugen

2. Wir definieren ein erstes Suchkriterium: `unter 4.09.100`

und wählen weitere Einschränkungen: **Suche weiter einschränken**

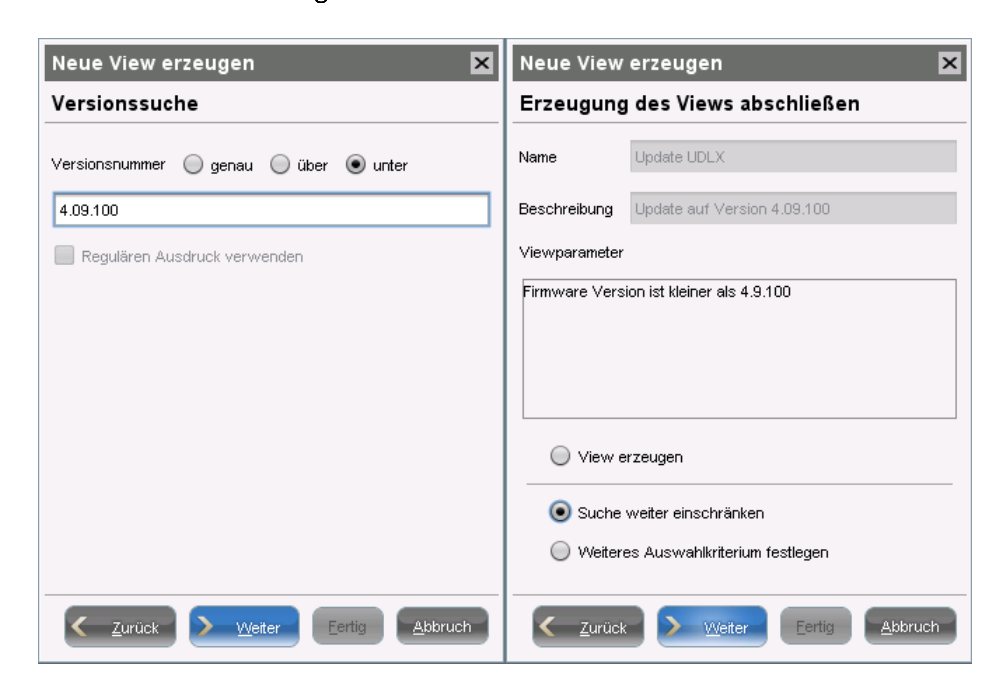


Abbildung 62: Versionssuche - View erzeugen

3. Als weiteren Suchparameter wählen wir **Produkt-ID**

   und als Suchkriterium definieren wir `UD.*LX` und aktivieren **Regulären Ausdruck verwenden**.

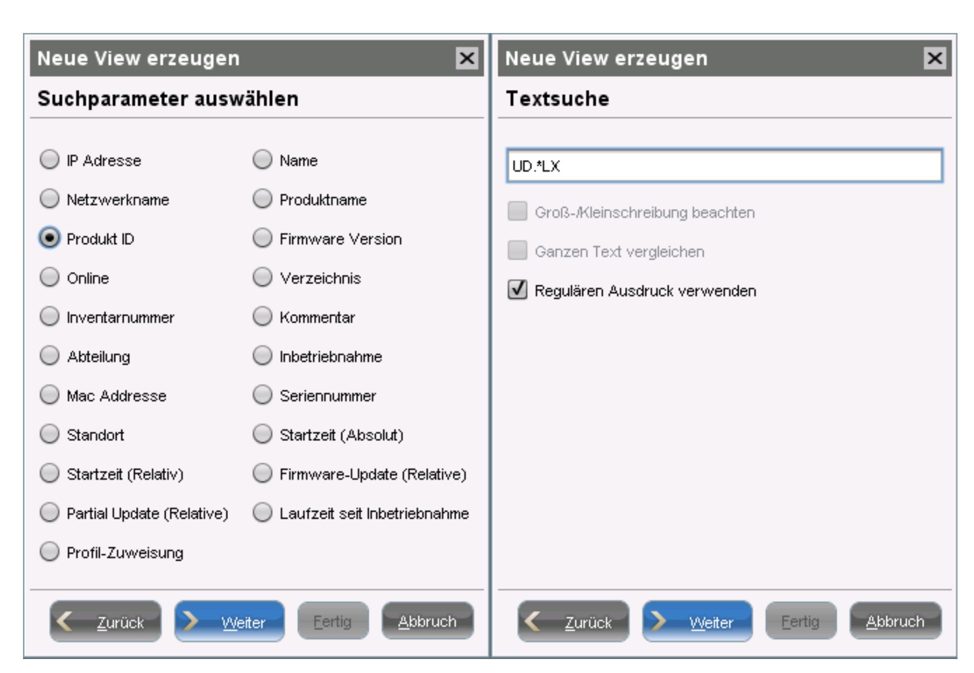


Abbildung 63: Suchparameter - Textsuche

4. Wir aktivieren das Kontrollkästchen **View erzeugen** und klicken **Fertig**.

Das Ergebnis wird im Inhaltsbereich angezeigt.

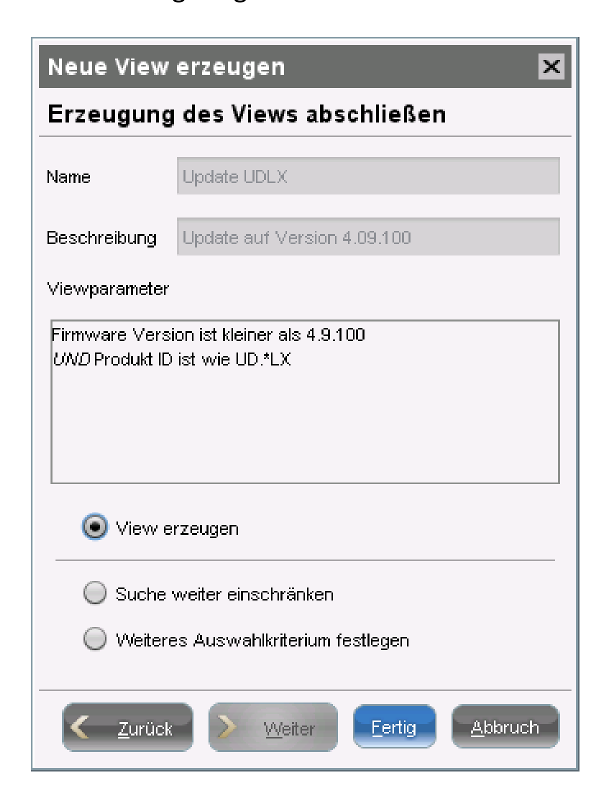


Abbildung 64: Ergebnisansicht einer View

5. In der Ergebnisansicht klicken wir auf **Bearbeiten**, um die angezeigten Daten zu konfigurieren.

Das Fenster **View bearbeiten** öffnet sich.

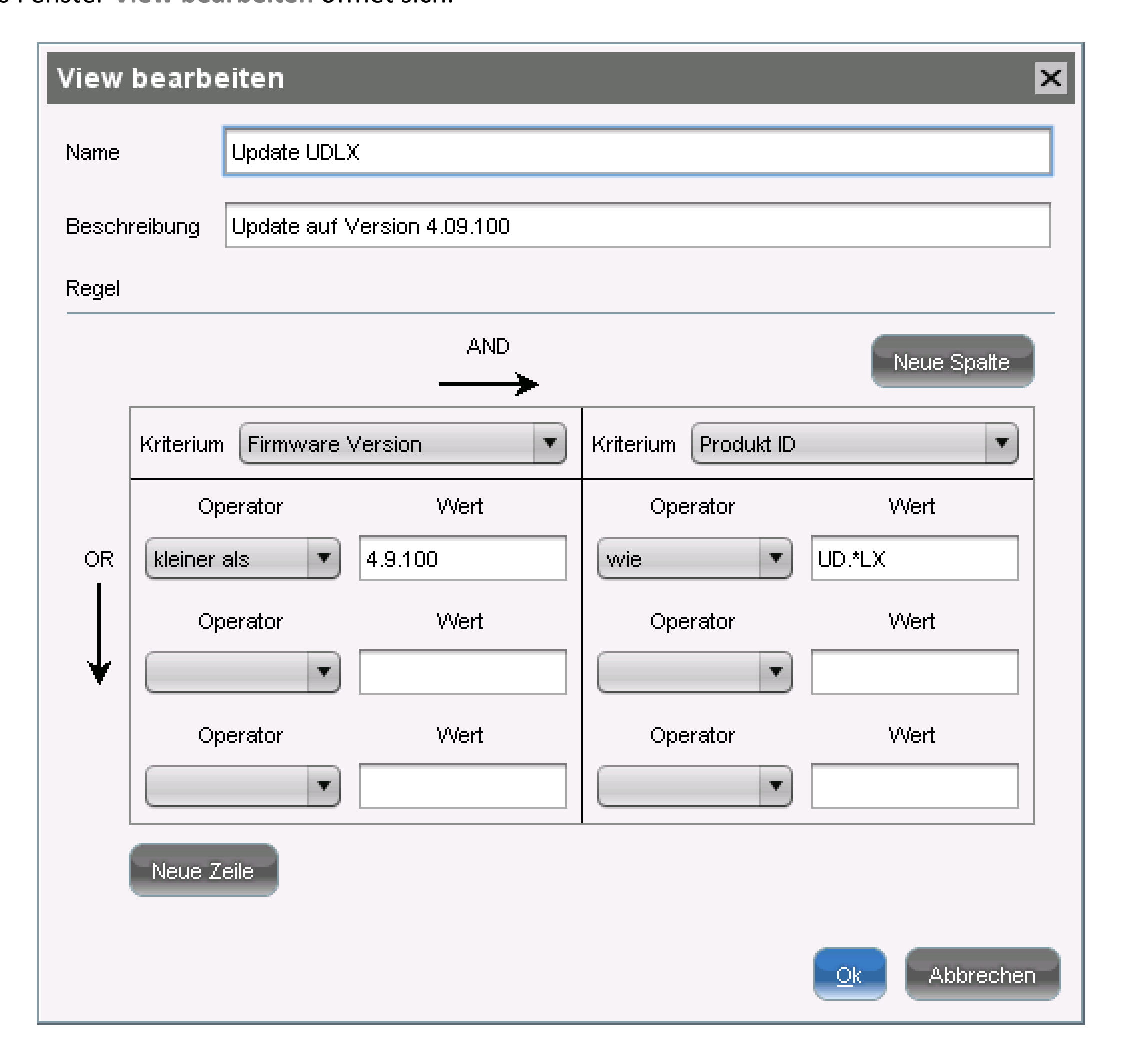


Abbildung 65: Der View-Expertenmodus

Wenn mehrere Filterkriterien einzugeben sind, können Sie am Anfang der Erstellung auch in den Expertenmodus wechseln. Diese Ansicht erlaubt Ihnen die schnelle logische (AND/OR) Verknüpfung mehrerer Kriterien und Werte.

7.2. View Ergebnisliste speichern

- Wählen Sie **Speichern unter** z. B. im Kontextmenü einer View, um die aktuelle Ergebnisliste einer View in einer Datei zu speichern. Für den Export stehen drei Dateiformate zur Verfügung: XML, HTML und XSL-FO.

Dies ist ein Beispiel für eine XML-Datei der obigen Ansicht:

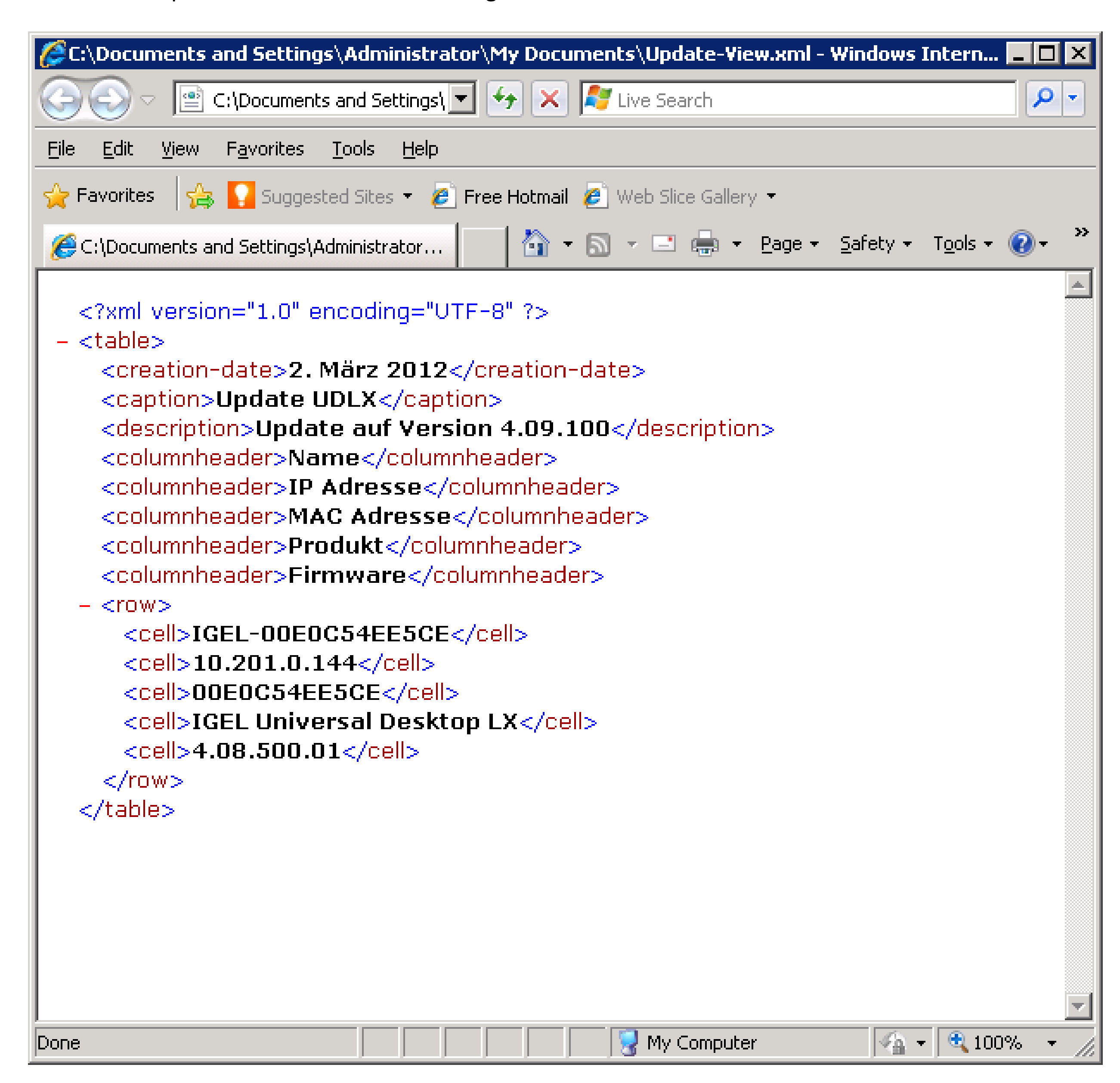


Abbildung 66: XML-Export der Ergebnisse

7.3. View per E–Mail verschicken

Das Verschicken von Mails funktioniert nur, wenn Sie geeignete *Mail-Einstellungen* (Seite 125) unter **UMS Administration→Konfiguration→Mail-Einstellungen** vorgenommen haben.

So verschicken Sie eine View per E-Mail:

1. Klicken Sie mit der rechten Maustaste auf eine **View**.
2. Wählen Sie im Kontextmenü **Sende View-Ergebnisse via Mail ...**
   Das Fenster **Sende View-Ergebnisse via Mail ...** öffnet sich.
3. Tragen Sie im Feld **Mail Recipient** die Empfängeradresse ein. Mehrere Empfängeradressen sind möglich, trennen Sie sie mit einem ";" (Strichpunkt) von einander.
4. Wählen Sie unter **Exportformat** das Format, in dem die View verschickt werden soll
5. Aktivieren Sie **Archiv erstellen**, um die View als Zip-komprimierte Datei zu verschicken.

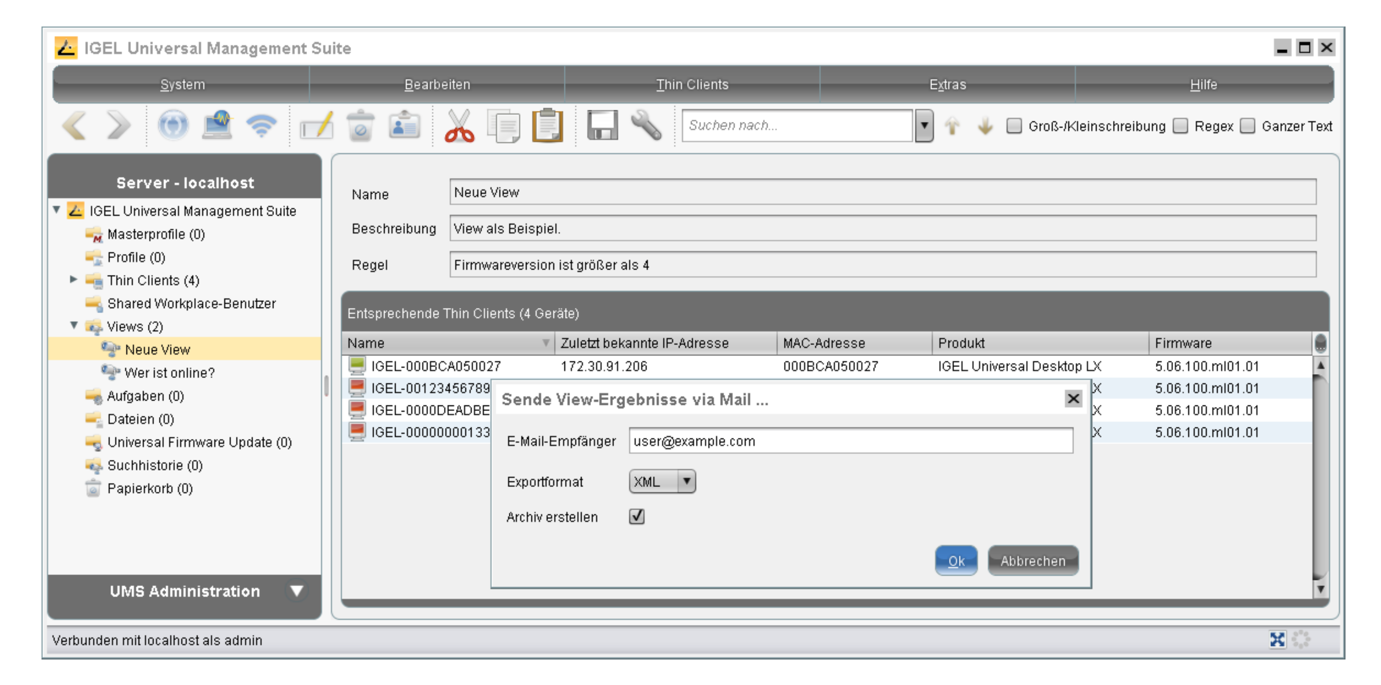


Abbildung 67: View-Ergebnisse via Mail verschicken

Sie können Views auch automatisiert und regelmäßig als *Administrative Aufgabe* (Seite 121) versenden.

8. Geplante Aufgaben

Der Aufgabenplaner dient dazu, die Ausführungszeit für bestimmte Thin Client-Befehle zu ermitteln. Diese Aufgaben können in Intervallen oder an bestimmten Wochentagen wiederholt werden.

So erhalten Sie eine Übersicht über alle bisher definierten geplanten Aufgaben:

➢ Wählen Sie einen Ordner aus der Unterstruktur **Aufgaben**.

Alle Aufgaben in diesem Ordner werden auf der rechten Seite des Fensters mit allen wichtigen Daten wie etwa dem auszuführenden Befehl, dem Datum und der Uhrzeit der nächsten Ausführung usw. angezeigt.

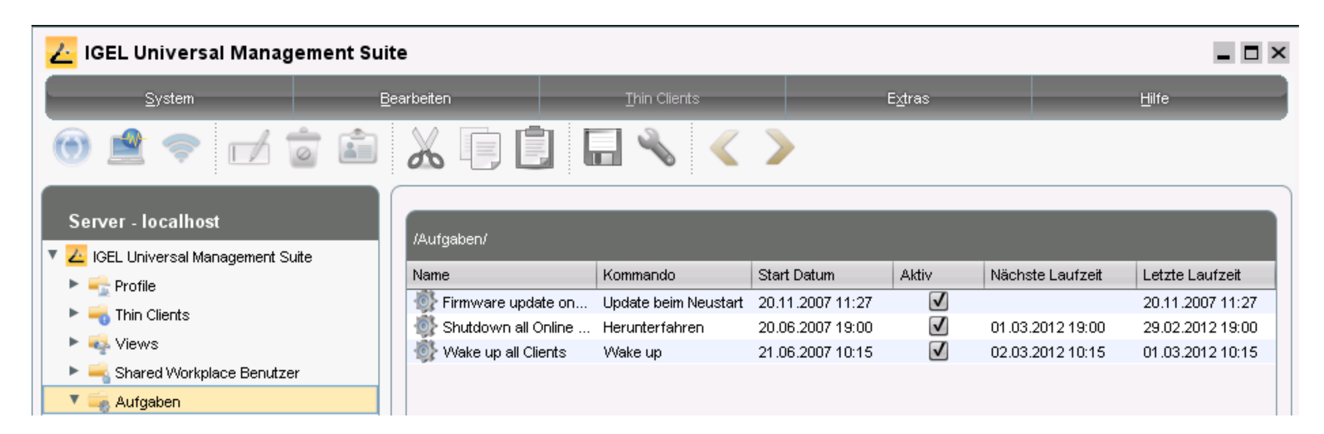


Abbildung 68: Übersicht geplanter Aufgaben

Über das Kontextmenü können Sie eine **Aufgabe bearbeiten**, **Umbenennen**, **Löschen** etc. und auch die bisherigen Ausführungsergebnisse löschen.

8.1. Neue Aufgabe anlegen

➢ Wählen Sie **Neue Aufgabe** aus dem Menü **Kontext** oder **System**.

Das Konfigurationsfenster enthält drei Registerkarten:

- **Details**
- **Zeitplan**
- **Zuordnung**

8.2. Kommandos für Aufgaben

Kommando	Beschreibung
Update	Führt das Firmwareupdate mit den bestehenden Einstellungen aus (Linux)
Herunterfahren	Fährt den Thin Client herunter
Neustart	Startet den Thin Client neu
Standby	Versetzt den Thin Client in den Standbymodus
Update beim Neustart	Führt das Firmwareupdate beim Neustart des Thin Clients aus (Linux)
Update beim Herunterfahren	Führt das Firmwareupdate beim Herunterfahren des Thin Clients aus (Linux)
Wakeup	Startet den Thin Client über das Netzwerk (Wake-on-LAN)
Einstellungen TC > UMS	Liest die lokale Konfiguration des Thin Clients in die UMS
Einstellungen UMS > TC	Sendet die Konfiguration der UMS an den Thin Client
Codecs laden	Lädt Codecs für den MPlayer (Linux, obsolet)
Codecs löschen	Entfernt Codecs des MPlayer (Linux, obsolet)
Flashplayer laden	Lädt das Flashplayer-Plugin für Firefox (Linux)
Flashplayer löschen	Entfernt das Flashplayer-Plugin für Firefox (Linux)
Firmwaresnapshot herunterladen	Führt das Firmwareupdate mit den bestehenden Einstellungen aus (WES)
Partielles Update	Führt das Partielle Update mit den bestehenden Einstellungen aus (WES)
Desktopanpassungen aktualisieren	Aktualisiert den eingestellten Bildschirmhintergrund und das Bootlogo (Linux)

8.3. Details

Name	Name der Aufgabe
Kommando	Befehl, der für alle zugewiesenen Thin Clients ausgeführt wird.
Start Datum/Ausführungszeit	Zeitpunkt der ersten Ausführung
Aktiv	Aufgaben lassen sich nach Bedarf aktivieren oder aussetzen.
Kommentar	Weitere Informationen zur Aufgabe
Ergebnisse sichern	Protokollierbare Ergebnisse werden in der Datenbank erfasst, dies ist nicht möglich für das Kommando `Wake-on-LAN`.
Max. Prozesse	Maximale Anzahl gleichzeitig ausgeführter Prozesse, diese werden somit ggf. blockweise ausgeführt.
Time-out	Wartezeit, die maximal vergeht, bis die UMS das Kommando an den nächsten Thin Client verschickt.
Verzögerung	Wartezeit, die minimal vergeht, bis die UMS das Kommando an den nächsten Thin Client verschickt.
Beim Booten neu versuchen	Parameter für das Updatekommando - ausgeschaltete Clients führen das Update beim nächsten Start durch.
ID-Aufgabe	Interne Aufgabennummer, die nicht bearbeitet werden kann. Bei einer neuen Aufgabe ist dieses Feld leer.
Benutzer	Name des UMS-Benutzers, der den Befehl ausführt.

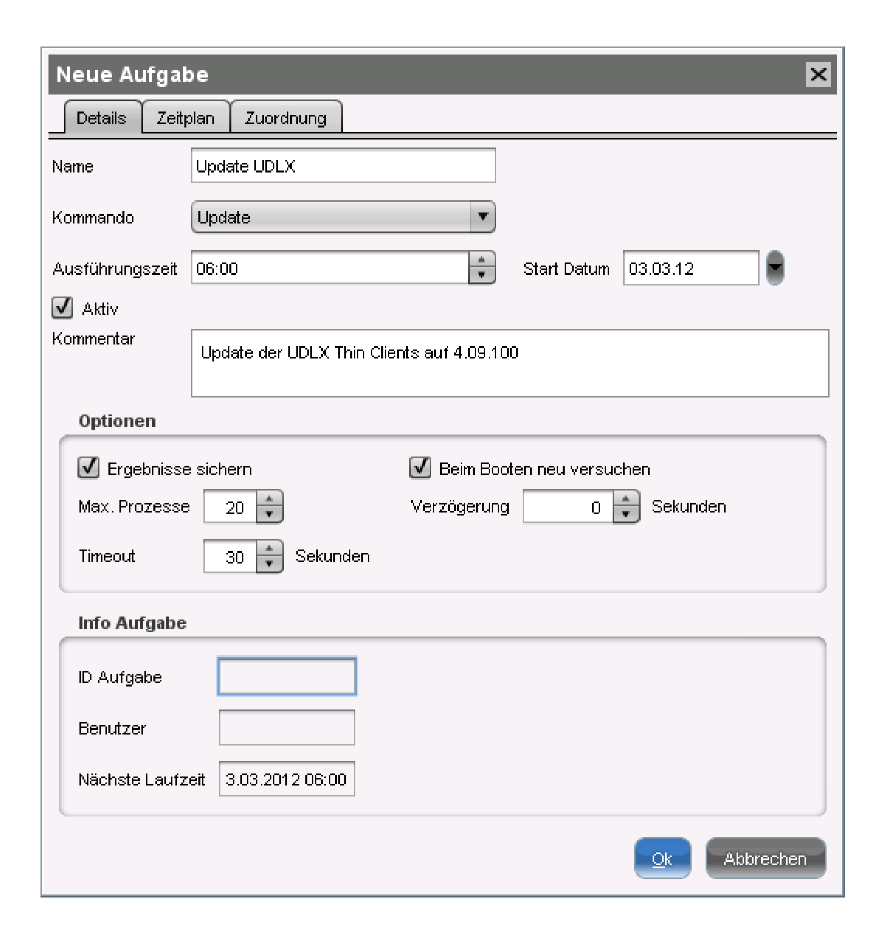


Abbildung 69: Details einer Aufgabe

8.4. Zeitplan

Start Datum/Ausführungszeit	Zeitpunkt der ersten Ausführung
Ablauf Datum/Uhrzeit	Nach diesem Zeitpunkt werden keine weiteren Kommandos ausgeführt.
Aufgabe wiederholen	Eine Aufgabe kann in festen Intervallen oder an bestimmten Tagen wiederholt werden. Feiertage lassen sich gesondert ausschließen. Die Liste der Feiertage pflegen Sie unter **Extras→Geplante Aufgaben→Feiertagslisten**.
Ausführung abbrechen	Bei wiederholter Ausführung können nicht fertiggestellte Aufgaben auch abgebrochen werden, es werden dann keine weiteren Kommandos an Thin Clients verschickt.

Die Optionen **Max. Prozesse, Verzögerung** und **Time-out** sind für alle Befehle sinnvoll, deren Ausführung länger dauert oder starken Netzwerkverkehr verursacht, z. B. das Herunterladen eines Firmware Updates, eines Codecs oder eines Snapshots. Um zu verhindern, dass viele Thin Clients gleichzeitig Daten von einem Dateiserver herunterladen, wird empfohlen, die Anzahl gleichzeitiger Threads zu reduzieren (z. B. auf 10) und eine Verzögerung (z. B. 1 Minute) einzurichten.

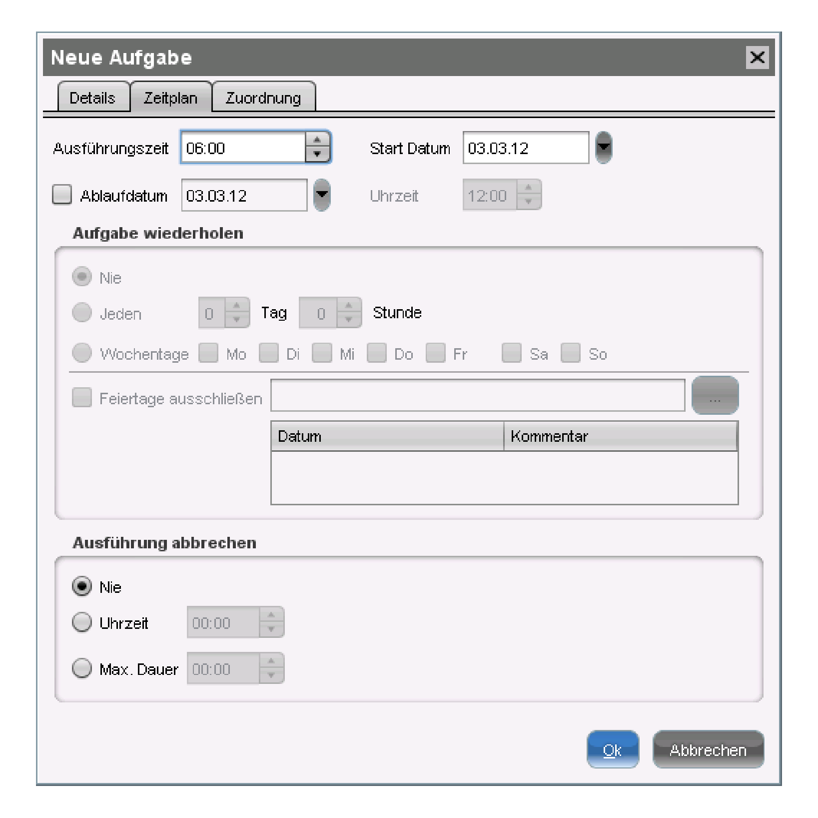


Abbildung 70: Zeitplan der Ausführung

8.5. Zuordnung

Über die **Hinzufügen** (+) können Sie fest bestimmten Thin Clients eine Aufgabe zuweisen.

Sie können auch ein Thin Client-Verzeichnis auswählen, dann wird die Aufgabe allen Geräten zugewiesen, die sich zum Zeitpunkt der Ausführung in diesem Verzeichnis befinden.

Die flexibelste Zuweisung erhalten Sie über die dynamische Geräteauswahl anhand einer ausgewählten View. Zum Ausführungszeitpunkt werden zunächst die Geräte über die Auswahlbedingungen der View ermittelt. Dann werden ihnen die Aufgaben zugewiesen.

Um eine statische Thin Client-Zuweisung durch die MAC-Adresse oder eine dynamische Zuweisung über das Verzeichnis oder die View zu erstellen, ist eine Schreibberechtigung für die entsprechenden Objekte erforderlich. Zum Zeitpunkt der Ausführung muss der Benutzer, der die Aufgabe erstellt hat, über die Schreibberechtigung für den betreffenden Thin Client verfügen. Dies muss berücksichtigt werden, wenn auch andere Benutzer eine Schreibberechtigung für eine Aufgabe haben, insbesondere wenn der Datenbankbenutzer eine Aufgabe erstellt hat.

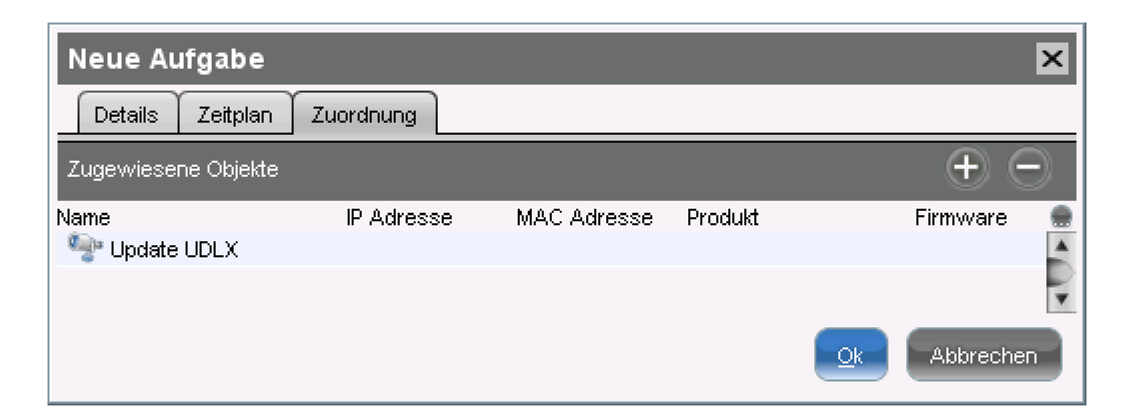


Abbildung 71: Aufgabenzuweisung über eine View

8.6. Ergebnisse

In der Ansicht einer fertig erstellten Aufgabe erscheint eine vierte Registerkarte: **Ergebnisse**. Hier erhalten Sie eine Übersicht des Status für eine Aufgabenausführung, aus der Sie über eine Drop-down-Liste auswählen können. Diese Ergebnisansicht lässt sich über zwei Schaltflächen löschen und aktualisieren. Folgende Statusmeldungen der Aufgabe -**Nachricht-** werden für die zugeordneten Thin Clients erfasst:

Wird ausgeführt Die Aufgabe wird gerade ausgeführt.

OK Die Aufgabe ist fertig gestellt, alle zugewiesenen Thin Clients wurden bearbeitet.

Zeit abgelaufen Die Aufgabe wurde abgebrochen, bevor alle zugewiesenen Thin Clients bearbeitet wurden, weil die Abbruchzeit oder die maximale Dauer erreicht worden sind.

Abgebrochen Die Aufgabe wurde aus unbekannten Gründen angehalten (z. B. Serverausfall).

Auch die Thin Clients selbst erhaltenen einen Status für die Aufgabenausführung:

Läuft Befehl wird gerade ausgeführt. Server wartet auf Antwort.

Wartet Die Aufgabe läuft, der Befehl wird ausgeführt, wenn der nächste Prozess verfügbar ist.

Übertragen Der Befehl wurde erfolgreich ausgeführt bzw. dem Thin Client übertragen.

Abgebrochen Aufgrund eines internen Fehlers oder einer unbekannten Ursache abgebrochen.

Fehlgeschlagen Befehl konnte nicht ausgeführt werden, Grund wird in der Meldungsspalte angezeigt.

Beim nächsten Booten Befehl wird beim nächsten Gerätestart ausgeführt.

Nicht bearbeitet Befehl wurde nicht ausgeführt, weil das Time-out der Aufgabe erreicht wurde.



Abbildung 72: Ausführungsstatus einer Aufgabe

9. Dateien

Durch eine **Dateiübertragung** können Sie Dateien im lokalen Dateisystem des Thin Clients speichern. Eine Datei muss auf einem UMS-Server registriert werden, bevor sie an den Thin Client gesendet werden kann. Beispiele sind lokal am Thin Client benötigte Virenscannersignaturen, Browserzertifikate, Lizenzinformationen etc.

9.1. Datei am UMS Server registrieren

Um eine Datei auf den Thin Client zu laden, muss sie zunächst auf dem UMS-Server registriert werden.

So registrieren Sie eine Datei auf dem UMS-Server:

1. Erstellen Sie mit dem UMS-Administrator eine Webressource, z. B. mit dem Namen `ums_filetransfer`.
2. Wählen Sie in der UMS-Konsole aus der Menüleiste **System→Neu→Neue Datei** oder gehen Sie im Navigationsbaum auf **Dateien** und wählen Sie im Kontextmenü **Neue Datei**.
3. Geben Sie unter **Datei Ursprung** den Pfad der zuvor erstellten Webressource zum Hochladen auf den UMS-Server an, indem Sie einen lokalen Pfad oder Serverpfad auswählen.
4. Wählen Sie unter **Klassifizierung**, ob die Datei mit oder ohne Browserzertifikat gespeichert werden soll.
5. Geben Sie unter **Thin Client-Speicherpfad** den Pfad auf dem lokalen Dateisystem des Clients an.
6. Vergeben Sie **Zugriffsrechte**.

   Diese werden der Datei bei der Übertragung an den Client mitgegeben und am Zielsystem angewendet.
7. Bestätigen Sie die Einstellungen mit **OK**.

   Die Datei wird jetzt in die Webressource kopiert und auf dem UMS-Server angemeldet.

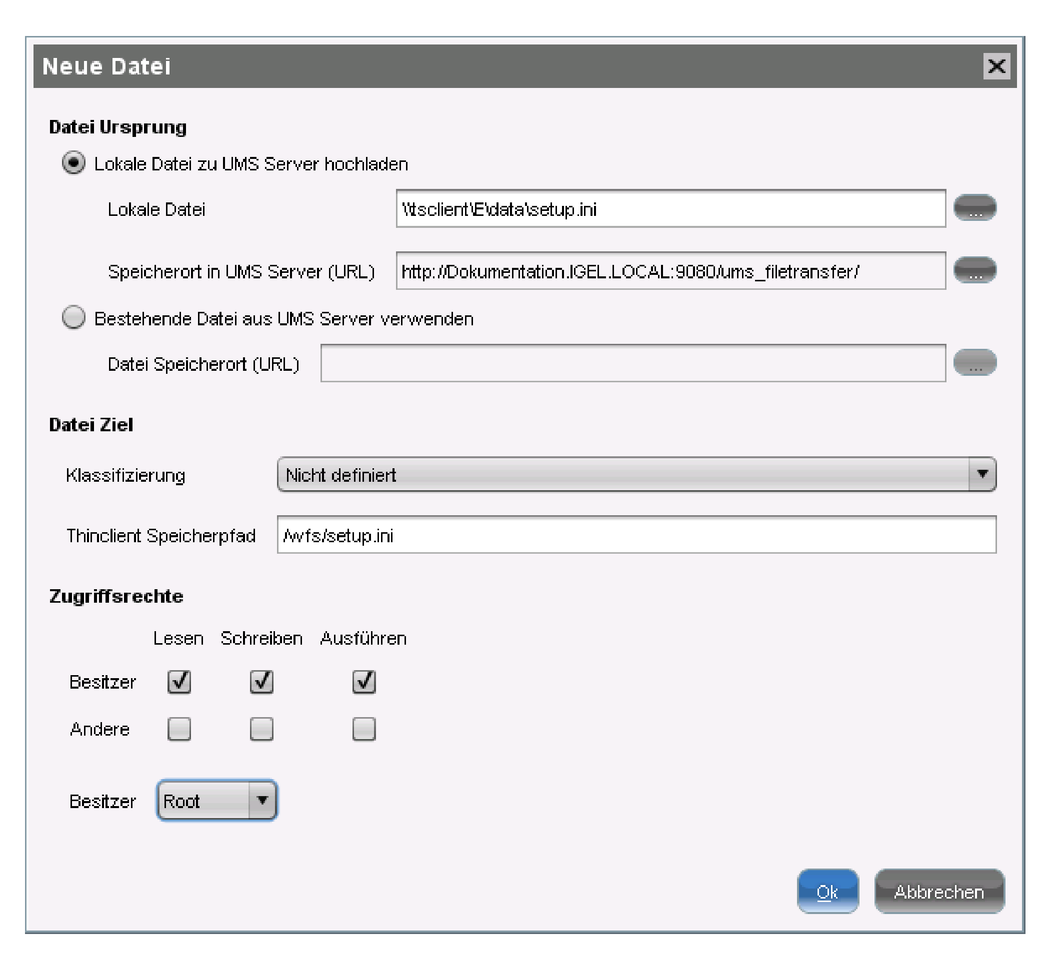


Abbildung 73: Neue Datei registrieren

9.2. Datei zum Thin Client übertragen

Um eine Datei auf einen Thin Client hochzuladen, muss sie einem Thin Client entweder direkt oder indirekt über ein Thin Client-Verzeichnis oder ein Profil zugewiesen werden.

➢ Ziehen Sie die Datei per Drag-and-Drop auf das Verzeichnis des Thin Clients

  oder integrieren Sie die Datei direkt im Thin Client im Fenster **Zugeordneten Objekte** über das **Hinzufügensymbol**, so wie sich auch Profile zuweisen lassen.
  Ist eine Datei einem Profil zugewiesen, dann wird sie mit den Profileinstellungen an die zugeordneten Clients übertragen.

Eine so zugewiesene Datei wird beim Übertragen der UMS-Einstellungen auf den Thin Client kopiert, z. B. während der Thin Client hochfährt. Solange die Datei dem Thin Client zugewiesen ist, wird sie mit der auf dem UMS-Server registrierten Datei synchronisiert, wenn z. B. die Datei `bookmarks.html` durch eine neue Version ersetzt wird. Die MD5-Prüfsumme der dem Thin Client zugewiesenen Datei wird mit der registrierten Datei verglichen. Wenn die Prüfsummen voneinander abweichen, wird die Datei erneut übertragen.

> Der Thin Client muss den UMS-Server mit seinem Full Qualified Domain Name (z. B. `mytcserver.mydomain.tld`) kontaktieren können.

Wenn eine Datei direkt auf dem Dateisystem (Webressource) ersetzt wurde, muss sie in der UMS-Konsole mit dem Befehl **Dateiversion aktualisieren** aus dem Kontextmenü der Datei aktualisiert werden. Der UMS-Server erkennt die Änderung in der Dateiversion sonst nicht.

9.2.1. Übertragung ohne Zuweisung

Eine auf dem UMS-Server registrierte Datei kann auch ohne Vorbereitung auf den Thin Client übertragen werden. Nutzen Sie dazu den Befehl **Datei zum Thin Client übertragen** aus dem Kontextmenü des Thin Clients, oder dem Thin Client-Menü in der Menüleiste. Die Datei muss dem Thin Client nicht zugewiesen werden.

Dies ist ein einfacher Dateikopiervorgang. Es erfolgt keine Dateiaktualisierung, wenn sich die Dateiversion auf dem UMS-Server ändert.

9.3. Datei vom Thin Client entfernen

So entfernen Sie eine Datei vom Thin Client:

- Löschen Sie die Zuweisung der Datei

  oder

- Entfernen Sie sie direkt mithilfe des Befehls **Datei vom TC löschen** aus dem Kontextmenü des Thin Client.

Wenn Sie eine Datei aus der Baumstruktur löschen, wird diese Datei von allen Geräten entfernt, denen sie zugewiesen wurde.

9.4. Datei auf den UMS Server übertragen

So laden Sie eine auf dem Thin Client vorhandene Datei in die Webressourcen herunter:

- Klicken Sie im Kontextmenü eines Thin Clients auf **Dateien→Datei TC→UMS**.

  Die UMS kann das lokale Dateisystem des Thin Clients nicht durchsuchen. Sie müssen den Speicherort und den Namen der Datei kennen, die Sie in die Webressource laden möchten.

> Eine vom Thin Client zu WebDAV übertragene Datei wird nicht automatisch auf dem UMS-Server registriert, sie befindet sich dann im Bereich des http-Servers der UMS. Sie können vorhandene Dateien aber nachträglich über **Neue Datei** registrieren.

Um die aktuelle lokale Konfiguration des Thin Clients auszulesen, müssen Sie die beiden lokalen Dateien `setup.ini` und `group.ini` über die IGEL Universal Management Suite kopieren:

1. Wählen Sie in der UMS-Konsole aus dem Kontextmenü des Thin Clients **Dateien→Datei TC→UMS**. Geben Sie als Quelle (Thin Client Speicherpfad) `/wfs/<Dateiname>` an.
2. Wählen Sie das Ziel auf dem UMS Server aus, z .B. `http://umsserver.domain:9080/ums_filetransfer/<Dateiname>`
3. Starten Sie die Dateiübertragung mit **Datei TC→UMS**.

10. Universal Firmware Update

Firmware Updates für alle IGEL-Thin Clients und Universal Desktop OS 2 (Universal Firmware Converter UDC2) sind auf dem öffentlichen IGEL-Server `http://myigel.biz` verfügbar. Innerhalb der UMS können Sie auf neue verfügbare Updates prüfen, diese herunterladen und sehr einfach an Thin Clients verteilen.

10.1. Servereinstellungen ändern

Der öffentliche Updateserver von IGEL ist vorkonfiguriert. Sollten Sie einen eigenen FTP-Server für die Verteilung der Updates einsetzen wollen, können Sie die Servereinstellungen entsprechend verändern:

1. Wechseln Sie in der UMS-Konsole im Bereich **Administration** zu **Globale Konfiguration→Universal Firmware Update**.
2. Klicken Sie **Editieren**.

   Das Fenster FTP Server Konfiguration bearbeiten öffnet sich.

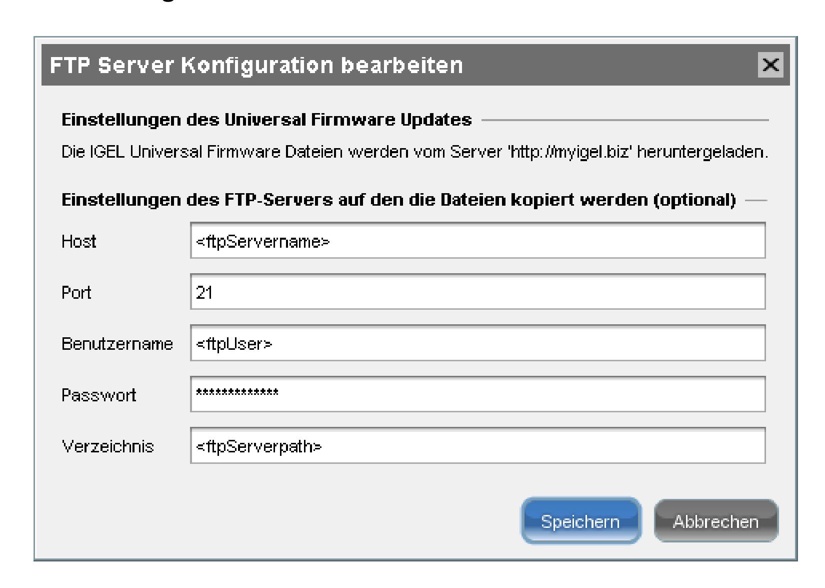


Abbildung 74: IGEL Universal Firmware Update

3. Verändern Sie die Einstellungen Ihres Servers.
4. Klicken Sie auf **Server Verbindung testen**, um die Kommunikation mit dem IGEL-Server und optional mit Ihrem eigenen FTP-Server zu überprüfen.

Ziel

Sie möchten einen HTTP-Proxy für den Zugriff auf den IGEL Update Server konfigurieren.

Lösung

So konfigurieren Sie die Proxyeinstellungen für Universal Firmware Update:

1. Rufen Sie die UMS-Konsole auf.
2. Wechseln Sie in den Administrationsbereich **Globale Konfiguration→Universal Firmware Update**.
3. Klicken Sie **Proxykonfiguration ändern**.
4. Aktivieren Sie die Verwendung des Proxys und geben Sie Ihre Verbindungsdaten ein.
5. Klicken Sie **Speichern** um die Einstellungen wirksam werden zu lassen.

10.2. Update suchen und herunterladen

So durchsuchen Sie den öffentlichen IGEL-Server nach Updates:

1. Klicken Sie im Navigationsbaum der Konsole mit der rechten Maustaste auf **Universal Firmware Updates**.
2. Wählen Sie aus dem Kontextmenü **Neue Updates suchen**.

   Es öffnet sich ein Fenster mit einer Liste aller Updates, die zu den in der UMS-Datenbank registrierten Firmwareversionen passen.

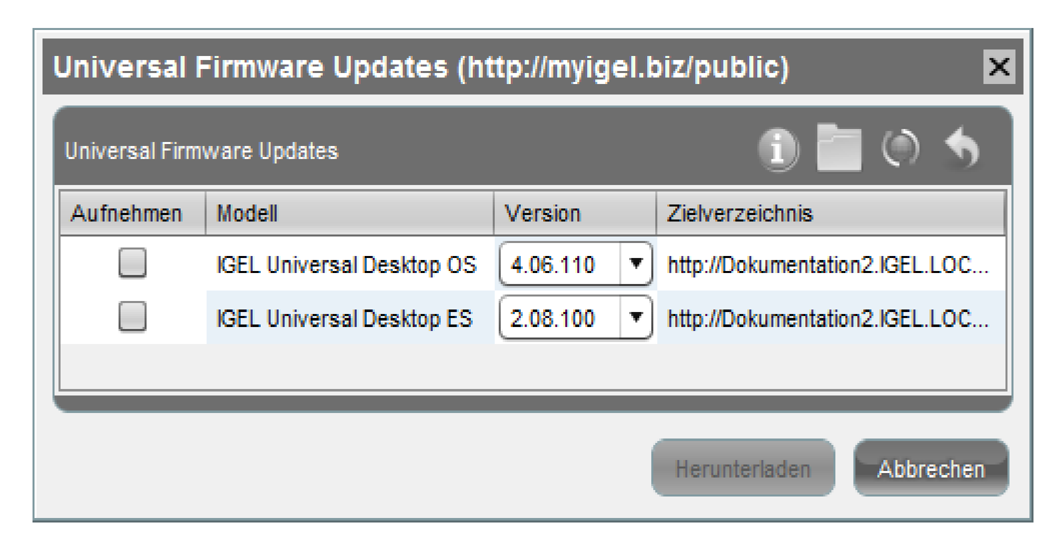


Abbildung 75: Verfügbare Updates auf dem Server

3. Klicken Sie auf **Information**, um sich die Releasenotes jedes Updates anzusehen.
4. Aktivieren Sie die Checkbox **Aufnehmen**, um die entsprechende Firmware herunterzuladen.

   Das Update wird zum Navigationsbaum hinzugefügt und der aktuelle Verarbeitungsstatus wird angezeigt.

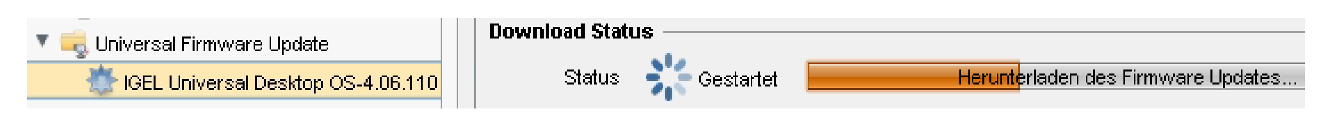


Abbildung 76: Status des Firmware Downloads

10.3. Von lokaler Quelle importieren

Sie können Updates auch von einer lokalen Quelle laden, z. B. von einem USB-Speicherstick.

Eine Firmware von einer lokalen Quelle hat nicht die Metainformationen wie sie auf dem IGEL-Server hinterlegt sind.

1. Wählen Sie aus dem Kontextmenü der Firmware Updates den Eintrag **Firmwarearchiv** aus.
2. Geben Sie einen Namen für die Anzeige des Updates in der UMS an.
3. Geben Sie ein Verzeichnis für die Ablage des Updates an, für die spätere Verteilung an Thin Clients.
4. Klicken Sie **OK** um den Import zu starten..

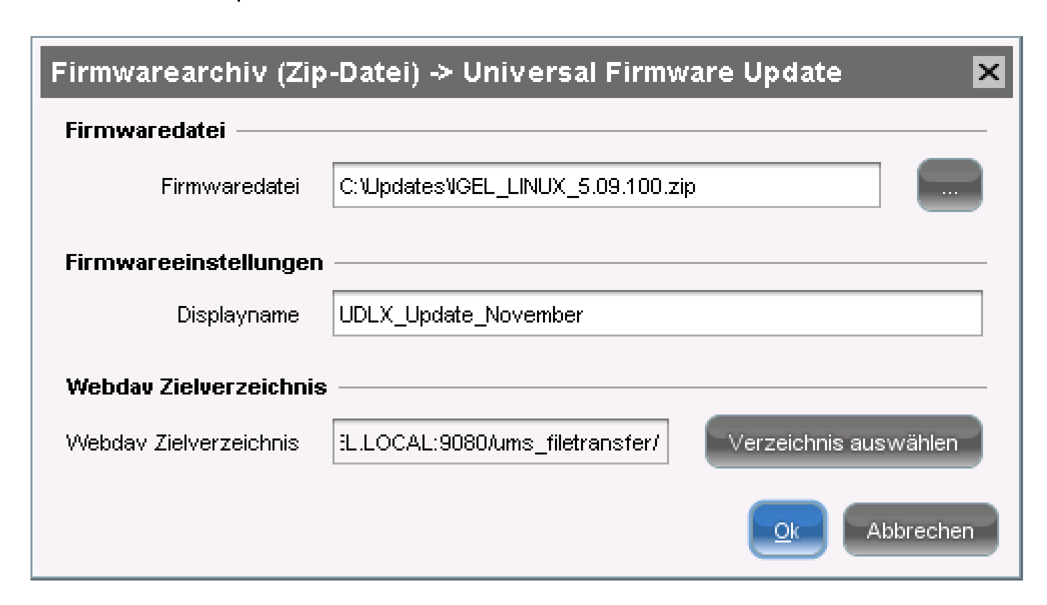


Abbildung 77: Update als ZIP oder SNP importieren

10.4. Aus dem UMS WebDAV importieren

Sie können auch einen zuvor erstellten und in einer Webressource abgelegten Snapshot eines Windows Embedded Standard-Thin Clients als Universal Firmware Update registrieren:

1. Wählen Sie **Snapshot** aus dem Kontextmenü der **Universal Firmware Updates**.
2. Geben Sie das zu importierende Update an.

10.5. Update einem Thin Client zuweisen

So weisen Sie einem Thin Client ein registriertes Firmwareupdate zu:

direkt: per Drag-and-Drop

über **Zugeordnete Objekte** im Thin Client-Fenster

indirekt: über ein Verzeichnis

➢ Starten Sie den Updateprozess nach der Übergabe der Information an den Thin Client manuell oder als **Geplante Aufgabe**.

Durch die Zuweisung wird ein "verstecktes" Profil mit den notwendigen Updateinformationen erzeugt, nach denen der Thin Client sein Update durchführen kann. Am Thin Client erkennt man die Zuweisung eines Universal Firmware Updates daran, dass die zuvor ggf. schon definierte Konfiguration verändert wurde, das automatisch erzeugte Updateprofil hat Vorrang vor anderen Profilen des Thin Clients.

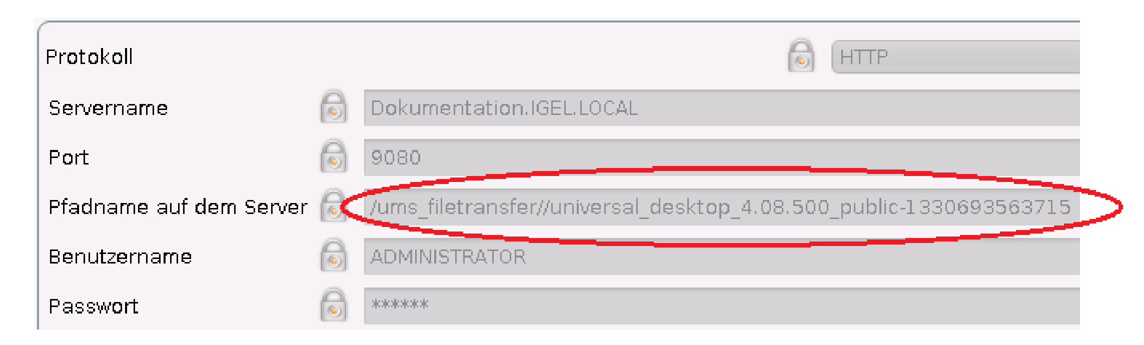


Abbildung 78: Automatisch erzeugtes Updateprofil

Die Zuweisung eines Updates startet noch nicht den Updateprozess, es werden nur die für das Update notwendigen Informationen an den Thin Client übergeben.

11. Zertifikate verwalten

11.1. Installation von Serverzertifikaten

Die IGEL UMS speichert auf jedem von ihr kontrollierten Thin Client ein Zertifikat. Dieses Zertifikat verhindert den unbefugten Zugriff auf die Thin Client-Konfiguration. Während der Installation wird ein eindeutiges Paar aus öffentlichem und privatem Schlüssel für jeden IGEL UMS-Server erzeugt. Der öffentliche Teil wird bei der Registrierung eines Thin Clients an der UMS automatisch an den Thin Client übertragen und dort gespeichert. Jeder Zugriff auf den Thin Client wird von diesem Zeitpunkt an mit dem privaten Schlüssel des Servers verglichen. Wenn andere IGEL UMS-Installationen versuchen, auf den Thin Client zuzugreifen, wird der Zugriff verweigert.

Sie können auch ein eigenes Zertifikat in die UMS einspielen, lesen Sie dazu die Anleitung in *UMS Netzwerk* (Seite 117).

11.2. Zertifikat entfernen

UMS sieht auch die Möglichkeit vor, das Zertifikat: von Thin Clients zu entfernen. Das kann erforderlich sein

- um den Umzug eines Thin Clients aus der Test- in die Produktivumgebung vorzubereiten
- um den Austausch des Serverzertifikats vorzubereiten.

So entfernen sie das Zeritifkat:

➢ Wählen Sie **Zertifikat entfernen** unter **Thin Clients→Kommandos→Sonstiges**.

Nun kann jeder IGEL UMS-Server auf die Thin Client-Konfiguration zugreifen, bis einer der Server den Client registriert.

11.3. Zertifikat speichern

Sie haben auch die Möglichkeit, das Zertifikat auf einem Client zu speichern, der bereits in der Datenbank registriert ist. Dies kann besonders dann sinnvoll sein, wenn das Zertifikat manuell vom Thin Client gelöscht worden ist.

So speichern Sie ein Zertifikat auf dem Thin Client:

1. Wählen Sie eine Gruppe oder einen einzelnen Thin Client aus.
2. Wählen Sie **Zertifikat speichern** unter **Thin Clients→Kommandos→Sonstiges**.

Als Alternative können Sie den Thin Client auch neu registrieren.

11.4. Konsolenzertifikat importieren

Wenn Sie die IGEL UMS-Konsole auf einem anderen Computer installieren, müssen Sie das Zertifikat `<INSTALLDIR>\rmclient\cacerts` importieren.

- Kopieren Sie diese Datei auf eine Diskette,

  oder

- Speichern Sie diese Datei in einem freigegebenen Ordner, auf den vom Zielcomputer aus zugegriffen werden kann.

12. Administrationsbereich

Im Bereich UMS-Administration sind einige Konfigurationsoptionen zusammengefasst, die zuvor über den UMS-Administrator nur direkt am UMS-Server verfügbar waren, z. B. die Anbindung von **Active Directories** oder die Einrichtung der **Universal Firmware Updates**.

Auch neue Werkzeuge wie **Administrative Aufgaben** oder die **Statusansicht der Serverdienste** stehen hier zur Verfügung.

12.1. UMS Netzwerk

Der Knoten **UMS Netzwerk** zeigt Informationen zum derzeit verwendeten SSL-Zertifikat an.

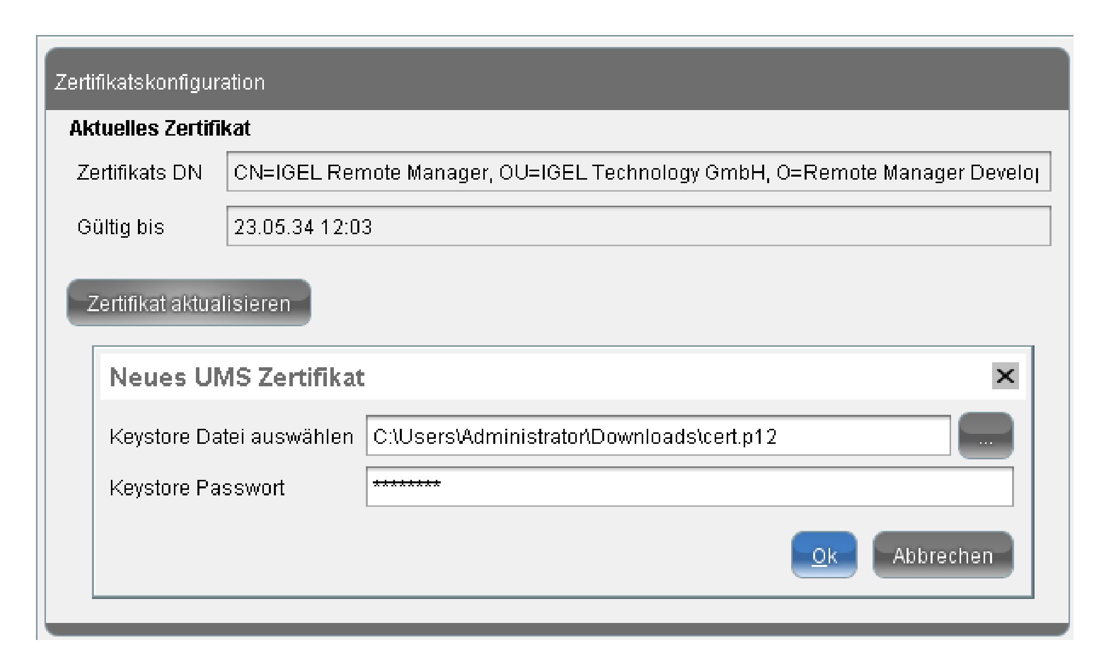
Daneben können Sie hier das bei der Installation erzeugte Zertifikat (selbstsigniert) durch ein eigenes SSL-Zertifikat ersetzen. Dieses muss dazu im Format PKCS 12 vorliegen.

> Falls Sie Zertifikate austauschen, erledigen Sie das, bevor Sie Thin Clients an UMS registrieren. Ansonsten müssen nach Sie einem Zertifikatswechsel die alten Zertifikate manuell *von den Thin Clients entfernen* (Seite 116).

So installieren Sie Ihr eigenes SSL-Zertifikat:

1. Klicken Sie die Schaltfläche **Zertfikat aktualisieren.**
2. Wählen Sie unter **Keystore Datei auswählen** Ihre Zertifikatsdatei aus.
3. Geben Sie im Feld **Keystore Passwort** das Passwort für Ihre Zertifikatsdatei ein.
4. Bestätigen Sie mit **OK**.

Die UMS Console fordert Sie anschließend zum Neustart des UMS Servers auf, um die Zertifikatsinstallation abzuschließen.



12.2. UMS–Server

Der Unterknoten **Server** listet alle zur Installation der UMS gehörenden Server und Load Balancer.

Bei einer Standardinstallation taucht hier in der Regel nur ein verfügbarer Server auf – in einem HA-Netzwerk werden alle installierten Server und Load Balancer angezeigt.

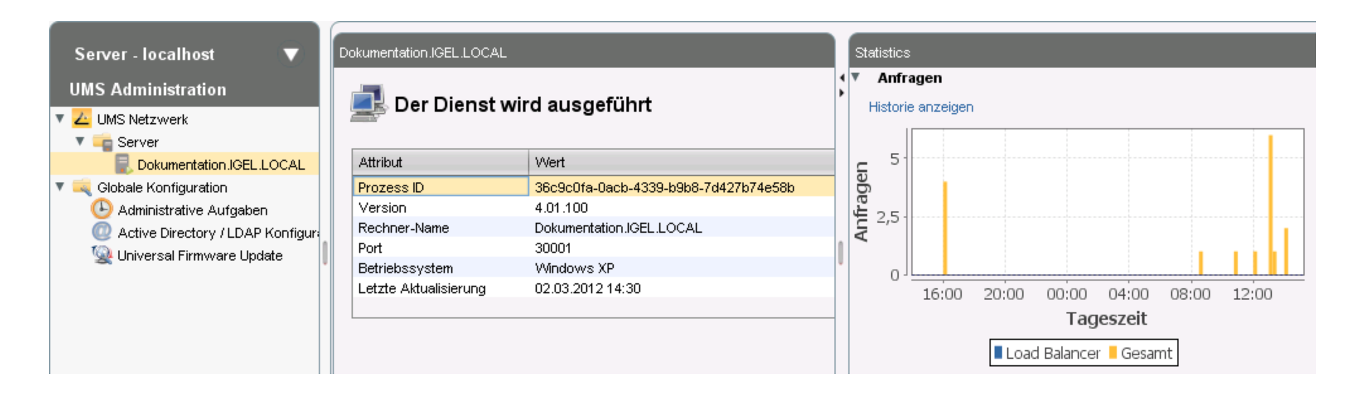


Abbildung 79: Status des UMS-Servers

Eine Übersicht der **Anfragen** und der **Abgewiesenen und wartenden Anfragen** durch Thin Clients erlaubt eine Einschätzung der Serverlast, wie sie sich über den betrachteten Zeitraum verteilt.

- Klicken Sie **Historie anzeigen**, um eine skalierbare Ansicht zu öffnen. Sie können mit der Maus in Ausschnitte hereinzoomen oder mittels Mausgeste (nach links ziehen mit gedrückter Maustaste) die Ansicht wiederherstellen.

12.3. Globale Konfiguration

Unter **Globale Konfiguration** regeln sie *Administrative Aufgaben* (Seite 119), Sie integrieren Benutzerdaten aus dem *Active Directory* (Seite 122), Sie richten das *Universal Firmware Update* (Seite 123) ein und verwalten die *Lizenzen* (Seite 123).

12.3.1. Administrative Aufgaben erstellen

Administrative Aufgaben erlauben die zeitgesteuerte und wiederkehrende Erstellung von Backups (nur interne Embedded-DB) und Bereinigung der Datenbank (unbenutzte Firmware entfernen, Cache erneuern, Logging-Informationen löschen).

So erstellen Sie eine neue **Administrative Aufgabe**:

1. Legen Sie über **Hinzufügen (+)** eine neue administrative Aufgabe an.
2. Geben Sie der Aufgabe einen **Namen**.
3. Wählen Sie unter **Aktion** die Art der Aufgabe (Backup oder Firmware entfernen).
4. Fügen Sie bei Bedarf eine ausführlichere **Beschreibung** hinzu.

In dieser ersten Ansicht lassen sich Aufgaben auch zunächst inaktiv setzen, um sie erst später zu aktivieren.

Geplantes Backup (Embedded-DB) erstellen

So erstellen Sie ein geplantes Backup

1. Geben Sie das **Verzeichnis** auf dem Server an, in welchem das erstellte Backup (`.embak`) abgelegt werden soll.
2. Klicken Sie **Weiter**.
3. Ordnen Sie die Aufgabe einem **Server** zu.

   > Bei Verwendung der Embedded DB kann es nur einen verbundenen Server geben, diese Auswahl ist somit fest dem einzigen Server zuzuweisen.

4. Klicken Sie **Weiter**.
5. Definieren Sie die Zeit der ersten Ausführung sowie ggf. ein Intervall für die **Wiederholung**, z. B. wöchentlich am Sonntag.

   Feiertage lassen sich wie bei **Geplanten Aufgaben** ausschließen.

6. Klicken Sie **Fertig**, um die Konfiguration der Aufgabe abzuschließen.



Abbildung 80: Ausführungszeitpunkt der Aufgabe

Unbenutzte Firmware entfernen

So löschen Sie regelmäßig Firmwareversionen aus der Datenbank, die nicht mehr benötigt wird:

1. Wählen Sie diese **Aktion** für eine **neue administrative Aufgabe**.
2. Klicken Sie **Weiter**.
3. Ordnen Sie die Aufgabe einem **Server** zu.

Im UMS-HA-Netzwerk kann nur jeweils ein Server eine Aufgabe durchführen.

4. Klicken Sie **Weiter**.
5. Definieren Sie die Zeit der ersten Ausführung sowie ggf. ein Intervall für die **Wiederholung**, z. B. wöchentlich am Sonntag.

   Feiertage lassen sich wie bei **Geplanten Aufgaben** ausschließen.
6. Mit **Fertig** schließen Sie die Konfiguration der Aufgabe ab.

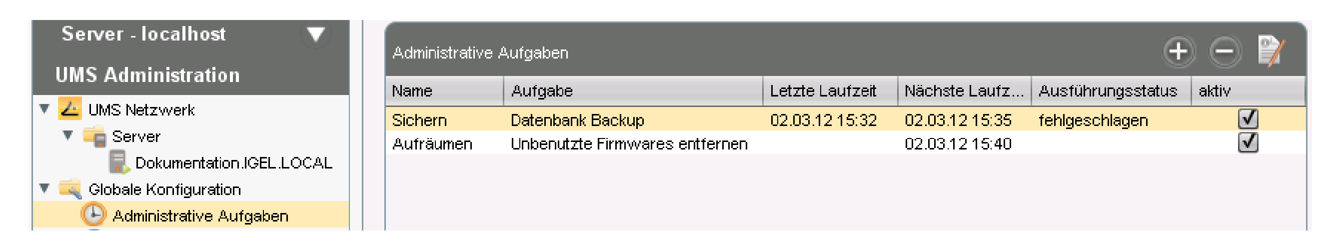


Abbildung 81: Statusmeldungen der Aufgaben

Caches erneuern

Diese Aufgabe erneuert zum definierten Zeitpunkt oder regelmäßig den Cache des UMS-Servers. Den Cache selbst konfigurieren Sie unter **Globale Konfiguration→Cache-Konfiguration**.

Logging Informationen löschen

Löscht die bereits angelegten Nachrichten- und Ereignis-Logs der UMS. Sie können für diese Aufgabe ein Zielverzeichnis für die Sicherung der Loggingdaten angeben, bevor das Log auf dem UMS-Server gelöscht wird.

> Die Logs des *Sicheren Spiegelns* (Seite 55) werden durch diese Administrative Aufgabe nicht gelöscht.

Thin Clients löschen

Diese Aufgabe löscht zum gewünschten Zeitpunkt alle Thin Clients aus der UMS-Datenbank, die zur Laufzeit die Kriterien einer View erfüllen (z.B. "alle Thin Clients, die länger als ein Jahr nicht gestartet wurden").

Export der View-Ergebnisse via Mail

> Das Verschicken von Mails funktioniert nur, wenn Sie geeignete *Mail-Einstellungen* (Seite 125) unter **UMS Administration→Konfiguration→Mail-Einstellungen** vorgenommen haben.

So richten Sie den regelmäßigen Mail-Versand einer View ein:

1. Wählen Sie **Export der View-Ergebnisse via Mail** im Fenster **Eine neue administrative Aufgabe anlegen**
2. Wählen Sie eine View über die Schaltfläche **View-ID→[...]** aus.
3. Wählen Sie die gewünschten Datenfelder unter **Konfiguration sichtbarer Spalten→[...]** aus.

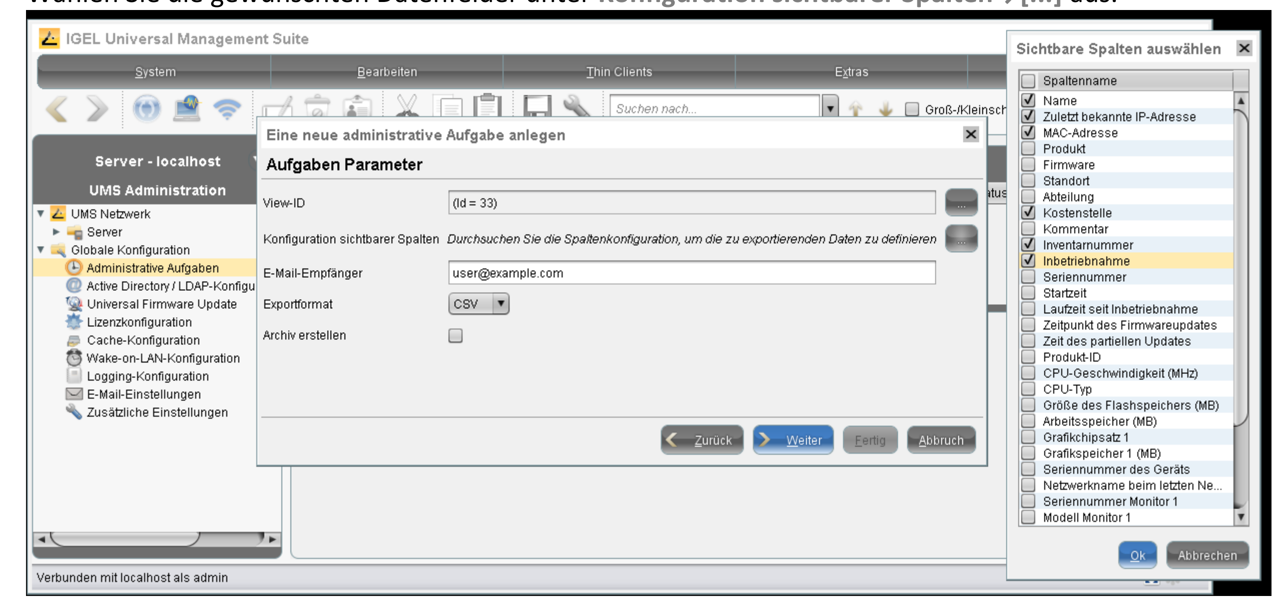


Abbildung 82: View und Spalten auswählen

4. Tragen sie die Empfängeradresse ein. Mehrere Empfängeradressen sind möglich, trennen Sie sie mit einem ";" (Strichpunkt) von einander.

5. Wählen Sie das **Exportformat** und ob die Datei gezippt werden soll
6. Im nächsten Fenster stellen Sie **Start** und **Ende**, Häufigkeit sowie die **Wochentage** der Ausführung ein. Einzelene Feiertage können sie gezielt ausschließen.



Abbildung 83: Ausführungszeit einstellen

7. Schließen Sie Ihre Eingaben mit der Schaltfläche **Fertig** ab.

12.3.2. Active Directory / LDAP einbinden

Die Anbindung des UMS-Servers an ein bestehendes Active Directory kann aus zwei Gründen sinnvoll sein:

- Sie möchten Benutzer aus dem AD als UMS-Administratorkonten importieren.
- Sie möchten Benutzerprofile über IGEL Shared Workplace einsetzen.

Für beide Einsatzzwecke müssen Sie die jeweiligen Active Directories zuvor im Administrationsbereich unter **Globale Konfiguration→Active Directory / LDAP Konfiguration** einbinden.

1. Fügen Sie über **Hinzufügen (+)** einen neuen Eintrag zur Liste der angebundenen Active Directories hinzu.
2. Geben Sie den Namen der **Domäne** an, den **Domain Controller** sowie die **Seitengröße**.

   Die Seitengröße ist eine serverseitige Begrenzung der Treffermenge von Objekten im Active Directory, Standardwert ist `1000`. Ändern Sie diesen Wert entsprechend Ihrer Serverkonfiguration.
3. Klicken Sie auf **Verbindung testen**, um die Anbindung nach Eingabe gültiger Benutzerdaten zu prüfen.

Es lassen sich mehrere Active Directories anbinden. Achten Sie daher beim Log-in, z. B. an der UMS-Konsole, auf die Angabe der korrekten Domäne.

In diesem Dokument werden die Begriffe Active Directory und LDAP z.T. synonym verwendet:

- Administrative Benutzer / UMS Administratoren lassen sich sowohl aus einem AD wie auch aus einem LDAP heraus importieren.
- Shared Workplace Benutzer können sich lediglich gegenüber einem Active Directory authentifizieren, ein LDAP-Dienst kann hierfür nicht verwendet werden.

12.3.3. Universal Firmware Update

Die Einrichtung ist beschrieben im Kapitel *Universal Firmware Update* (Seite 112).

12.3.4. Lizenzkonfiguration

In diesem Bereich erhalten Sie einen Überblick über die Verfügbarkeit und den Status aller Lizenzen und eine Auflistung der Registrierungsdaten.

12.3.5. Cache-Konfiguration

Der Cache, oder auch Zwischenspeicher, ist in den UMS GUI-Server integriert, durch ihn soll die gesamte Performance verbessert werden, wenn der Thin Client seine Einstellungen abruft. Darüber hinaus kann die UMS die Thin Client-Einstellungen auch dann bereitstellen, wenn die UMS-Datenbank nicht läuft. Beachten Sie jedoch, dass Sie bei nicht aktivierter Datenbank keine Thin Client-Einstellungen ändern können.

Cache aktivieren	Cache aktivieren oder deaktivieren
Verwaiste Elemente löschen	Löscht Einträge im Cache, die nicht in der Datenbank gefunden werden können.
Alle Thin Clients hinzufügen	Wenn der Cache aktualisiert wird, können Sie die Einstellungen aller Thin Clients zum Cache hinzufügen, die der UMS bekannt sind. Ansonsten werden nur die Einstellungen der Thin Clients hinzufügt, die sich mindestens einmal mit der UMS des aktuellen Hosts verbunden haben.
Cache aktualisieren, wenn der Server gestartet wird	Der Cache wird beim Serverstart aktualisiert. Um detaillierte Aktualisierungsangaben zu machen, gehen Sie in die **UMS-Konsole** und klicken Sie auf **Administrative Aufgaben** in der **UMS-Administration**.

➢ Wählen Sie in der UMS-Konsole im Menü **Extras→Cache Verwalten**.

  Im Dialogfenster werden einige Details über den Cache angezeigt, z. B. welche Einträge sich im Cache befinden, wann die nächste Aktualisierung stattfindet usw.

Einige Cacheaktionen können Sie auch hier ausführen:

Cache aktualisieren	Aktualisiert sofort alle Cacheelemente
Cache leeren	Entfernt sofort alle Cacheeinträge
Ansicht aktualisieren	Liest die aktuelle Cacheinformation neu aus

Im Administrationsbereich der UMS-Konsole können Sie auch eine **Administrative Aufgabe** anlegen, um den Cache regelmäßig automatisch zu aktualisieren.

12.3.6. Wake-on-LAN-Konfiguration

Thin Clients lassen sich mittels MagicPacket über das Netzwerk aufwecken. In der UMS-Administration können Sie festlegen, an welche Netzwerkadressen diese Pakete verschickt werden. Standardmäßig werden sie als Broadcast und an die letzte bekannte IP des Thin Clients versendet.

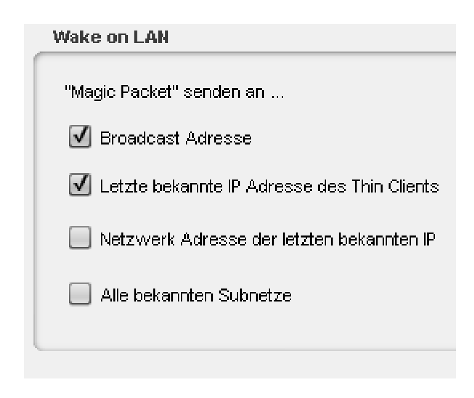


Abbildung 84: Wake-On-LAN Einstellungen

12.3.7. Logging

Sie können Logs zu zwei unterschiedlichen Bereichen anlegen:

Nachrichten-Log-Einstellungen:	Logging für vom Benutzer gestartete Aktionen
Ereignis-Log-Einstellungen:	Logging für vom Thin Client gestartete Aktionen

Unabhängig voneinander können sie jeden Logtyp

- aktivieren oder deaktivieren,
- für eine begrenzte Zeit oder eine begrenzte Anzahl von Einträgen oder unbegrenzt speichern,
- einrichten und die Aktionen steuern, die registriert werden sollen.

Einige Tipps für das Arbeiten mit Logs:

- Registrieren Sie Nachrichten zusätzlich mit Detailinformationen.
- Protokollieren Sie außerdem den Namen des UMS-Administrators, der die jeweilige Aktion ausgeführt hat.
- Zu protokollierende Aktionen schalten Sie in der Log-Level-Konfiguration ein oder aus.

Standardmäßig werden bei Aktivierung des Loggings alle Aktionen erfasst.

- Klicken Sie **System →Logging**, um sich das aktuelle Log und die exportierten Informationen in der UMS-Konsole anzeigen zu lassen.

  Dort ist auch ein manueller Export der Log-Information möglich.

> Im Administrationsbereich der UMS-Konsole können Sie auch eine **Administrative Aufgabe** anlegen, um die Logs regelmäßig automatisch zu sichern und zu löschen.

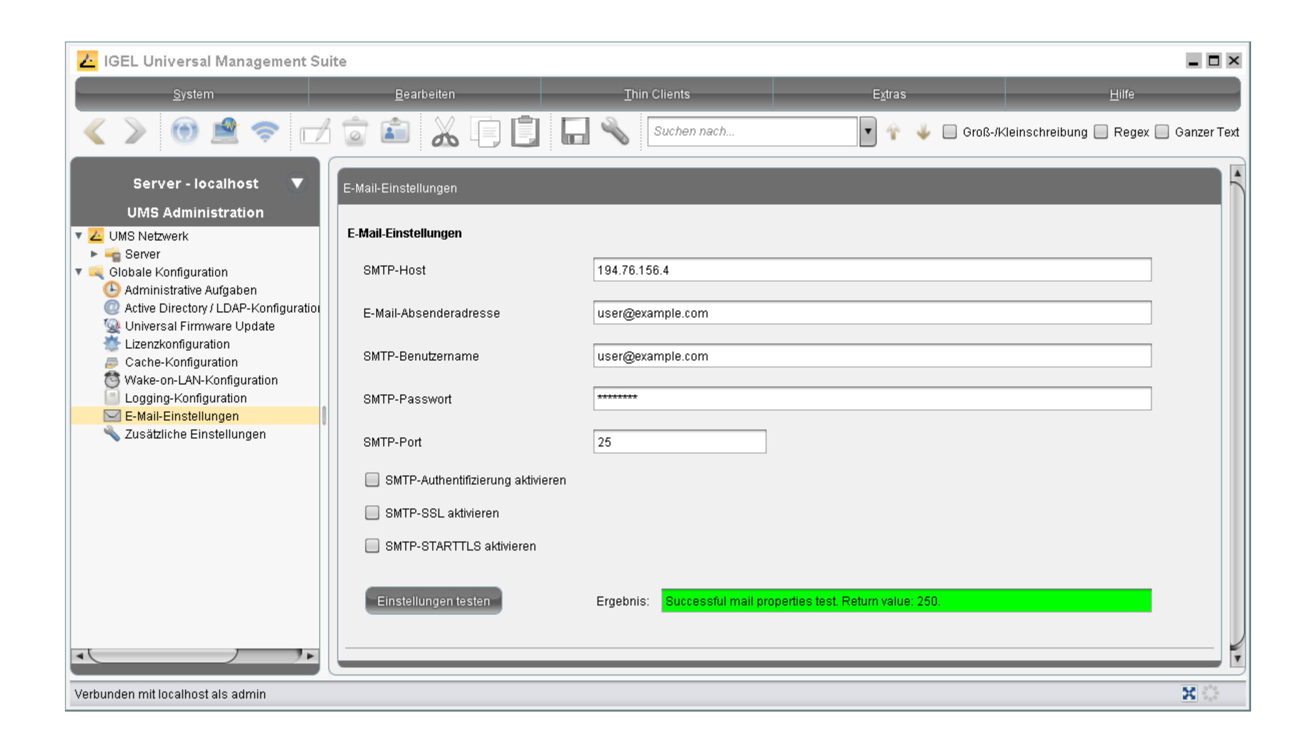
12.3.8. E-Mail-Einstellungen

> Die hier beschriebenen Mail-Einstellungen sind die Voraussetzung für die Funktionen *View per E-Mail verschicken* (Seite 102) und *Export der View-Ergebnisse via Mail* (Seite 121).

1. Öffnen Sie die Seite **UMS Administration→Globale Konfiguration→E-Mail-Einstellungen**.
2. Tragen Sie in das Feld **SMTP-Host** den im DNS bekannten Namen oder die IP-Adresse des SMTP-Servers (Postausgangsservers) ein.
3. Tragen Sie in das Feld E-**Mail-Absender-Adresse** den gewünschten Absender der E-Mails ein.
4. Legen Sie im Feld **SMTP-Benutzername** fest, mit welchem Benutzernamen sich die IGEL Universal Management Suite beim SMTP-Server anmelden soll.
5. Tragen Sie in das Feld **SMTP-Passwort** das Passwort für den SMTP-Benutzer ein.
6. Tragen Sie in **SMTP-Port** ein, mit welchem Port das Servers sich die IGEL Universal Management Suite verbinden soll. Bei unverschlüsseltem SMTP ist das Port 25, beim Einsatz von SMTP-SSL der Port 465.
7. Wählen Sie **SMTP-Authentifizierung aktivieren, SMTP-SSL aktivieren** oder **SMTP-STARTTLS aktivieren**, falls der SMTP-Server eine dieser Optionen einsetzt. Sehen Sie in der Dokumentation Ihres E-Mail-Anbieters nach, welche Methoden er unterstützt. Falls Sie zum Versand ein Gmail-Konto verwenden möchten, lesen Sie die **Best Practice Mail Settings for Gmail Accounts.**

8. Überprüfen Sie Ihre Einstellungen durch Klicken der Schaltfläche **Einstellungen testen.** Bei Erfolg färbt sich der Ergebnisbalken grün, andernfalls rot.

Abbildung 85: E-Mail-Einstellungen



Einstellungen für das Verschicken von E-Mails per Gmail (Google Mail) finden Sie in einer *Best Practice* (*http://edocs.igel.com/index.htm#10202904.htm*).

12.3.9. Zusätzliche Einstellungen

Hier finden sich weitere, globale Parameter:

- **Papierkorb aktivieren**: Aktiviert den UMS-*Papierkorb* (Seite 38).
- **Sicheres VNC global aktivieren:** Erlaubt ausschließlich *Sicheres Spiegeln* (Seite 55) für alle Thin Clients, die dies unterstützen.
- **Benutzernamen im VNC-Log speichern**: Erweitert das Log des *Sicheren Spiegelns* (Seite 55) um den Benutzernamen.
- **Templateprofile aktivieren:** Schaltet die Unterstützung für *Templateprofile* (Seite 83) ein.
- **Masterprofile aktivieren:** Ermöglicht das Verwenden von *Masterprofilen* (Seite 78).

13. Active Directory Benutzer importieren

Der Import von Benutzern aus dem Active Directory in die UMS-Konsole erfolgt in drei Schritten:

- Anmeldung am Active Directory
- Auswahl der zu importierenden Benutzer und Start des Imports
- Protokoll des Importprozesses

So importieren Sie Benutzer aus dem Active Directory in die UMS-Konsole:

1. Starten Sie den Importdialog der UMS-Konsole über **System→Administratorkonten→Importieren**.
2. Melden Sie sich am AD/LDAP-Service an.

   Die Anbindung ist *oben* (Seite 122) beschrieben. Nur angebundene ADs stehen zur Auswahl für den Import von Benutzerkonten.



Abbildung 86: AD-Anmeldung

3. Klicken Sie **Weiter**.

   Es öffnet sich der Active Directory-Browser.
4. Wählen Sie einzelne Benutzer oder Gruppen aus dem Navigationsbaum Ihres ADs aus.

   Die markierten Benutzer/Gruppen lassen sich über das Kontextmenü oder per Drag-and-Drop in die zu importierende Auswahl übernehmen bzw. wieder entfernen. Aus der Trefferliste **Gefundene AD Accounts** lassen sich die gefundenen Benutzer/Gruppen über die Symbole in die Liste **Ausgewählte Accounts** übertragen.

Eine Mehrfachauswahl verschiedener Benutzer und Gruppen ist möglich.

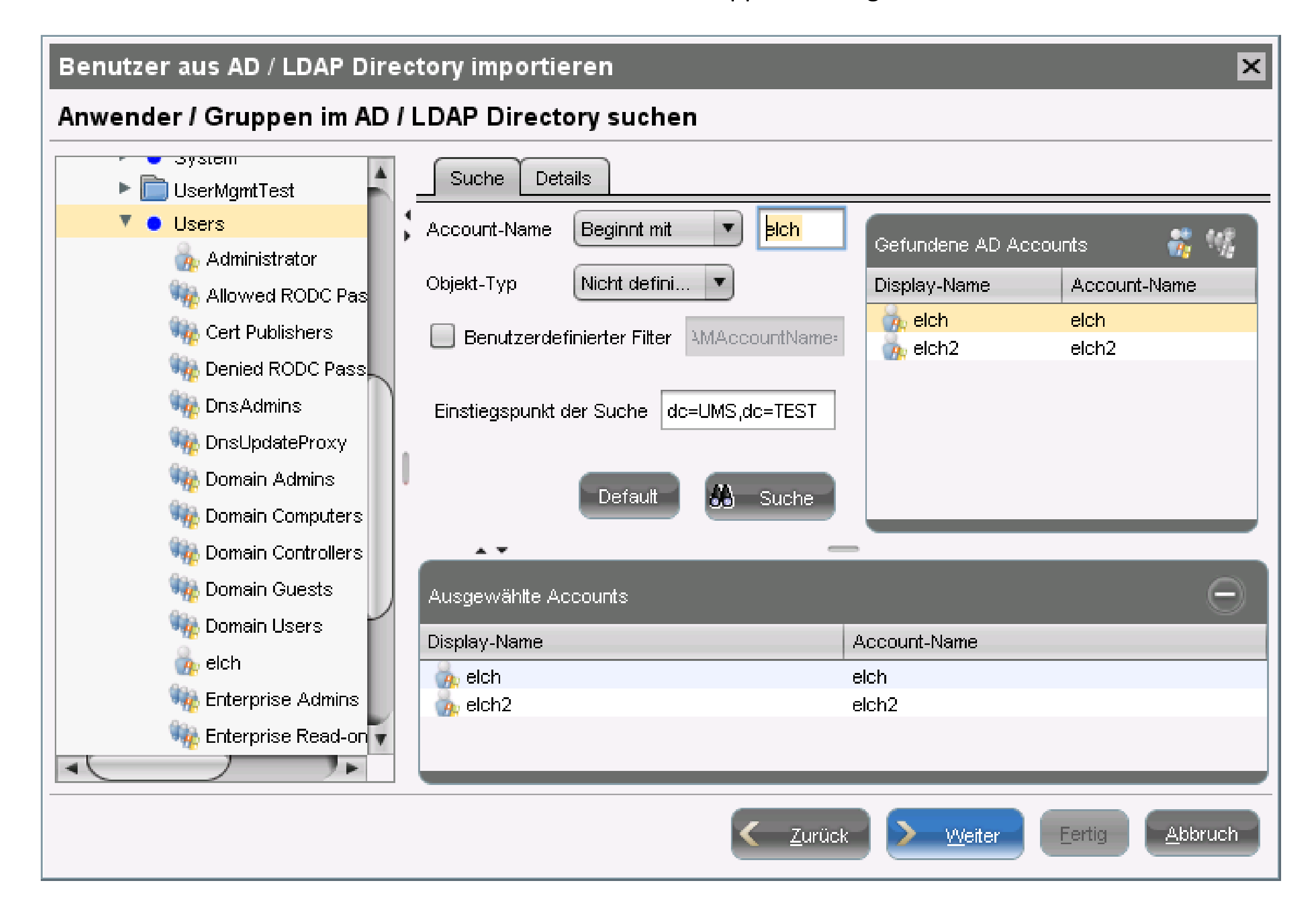


Abbildung 87: AD-Import-Filter

Alternativ zur Navigation im Navigationsbaum lassen sich Benutzer oder Gruppen auch über die **Suche** selektieren und der Auswahl hinzufügen.

5. Klicken Sie **Weiter** um den Import zu starten.

   Ein Bestätigungsfenster öffnet sich.

Der erfolgreiche Import eines Benutzers kann nicht rückgängig gemacht werden, Sie müssen den irrtümlich angelegten UMS-Administrator in der Verwaltung der Administratorkonten manuell löschen. Als Name des importierten AD-Benutzers wird in der IGEL UMS das **Konto** verwendet.

13.1. Symbolerklärung

Im AD-Navigationsbaum haben die Symbole folgende Bedeutung:

Benutzerkonto im Active Directory

Benutzergruppe im Active Directory

Der Auswahl hinzugefügtes Benutzerkonto

Der Auswahl hinzugefügte Benutzergruppe

Rechner im Active Directory

Organisationseinheit (OU) im Active Directory

Beliebiges Objekt, welches nicht Benutzer oder Gruppe ist

Das Kontextmenü erlaubt folgende Aktionen auf Baumelemente:

Benutzer (oder Gruppenmitglied) der Auswahl hinzufügen

Benutzergruppe der Auswahl hinzufügen

Element als Startpunkt für die Suche im AD setzen

Eigenschaften (Details) des Elements anzeigen

Einige Tipps:

- Durch Halten der Strg -Taste beim Drag-and-Drop einer Gruppe werden die Gruppenmitglieder ausgewählt und nicht die Gruppe an sich.
- Wird eine Organisationseinheit ausgewählt, werden nur die Mitglieder hinzugefügt, nicht die OU an sich.
- Die Tasten Einfg und Entf können zum Hinzufügen und Entfernen von Elementen der Auswahl verwendet werden.
- Ist ein Benutzer im UMS sowohl als Administrator als auch als Gruppenmitglied vorhanden, so überwiegen die Berechtigungen, die am Benutzer selbst hängen.

13.2. Suche im Active Directory

Im AD-Navigationsbaum haben die Optionen folgende Bedeutung:

Konto	Suche basierend auf Kontonamen bzw. Teilen davon
Objekttyp	Suche auf Benutzer oder Gruppen beschränken
Filter	Filterkriterien entsprechend des RFC-2254-Standards
Einstiegspunkt	Startelement im Baum, an welchem die Suche beginnt
Zurücksetzen	Setzt alle Suchoptionen auf die Standardwerte
Suche	Startet die eingestellte Suche

Das Kontextmenü erlaubt folgende Aktionen auf Elemente der Trefferliste:

- Benutzer (oder Gruppenmitglied) der Auswahl hinzufügen
- Benutzergruppe der Auswahl hinzufügen
- Eigenschaften des Elements anzeigen
- Tooltip (Objekteigenschaften bei Mouse-over) anzeigen

Sie können sich die Eigenschaften der für den Import ausgewählten Objekte nochmals über das Kontextmenü anzeigen lassen und eventuell Objekte vor dem Import entfernen.

13.3. Ergebnisliste des Imports

Im Anschluss an den Import öffnet sich ein Ergebnisfenster.

Hier wird angezeigt, wie viele Konten beim Import ignoriert wurden und welche Konten erfolgreich importiert wurden. Ist ein Benutzerkonto in der UMS bereits vorhanden, wird dieses AD-Konto beim Import übersprungen.

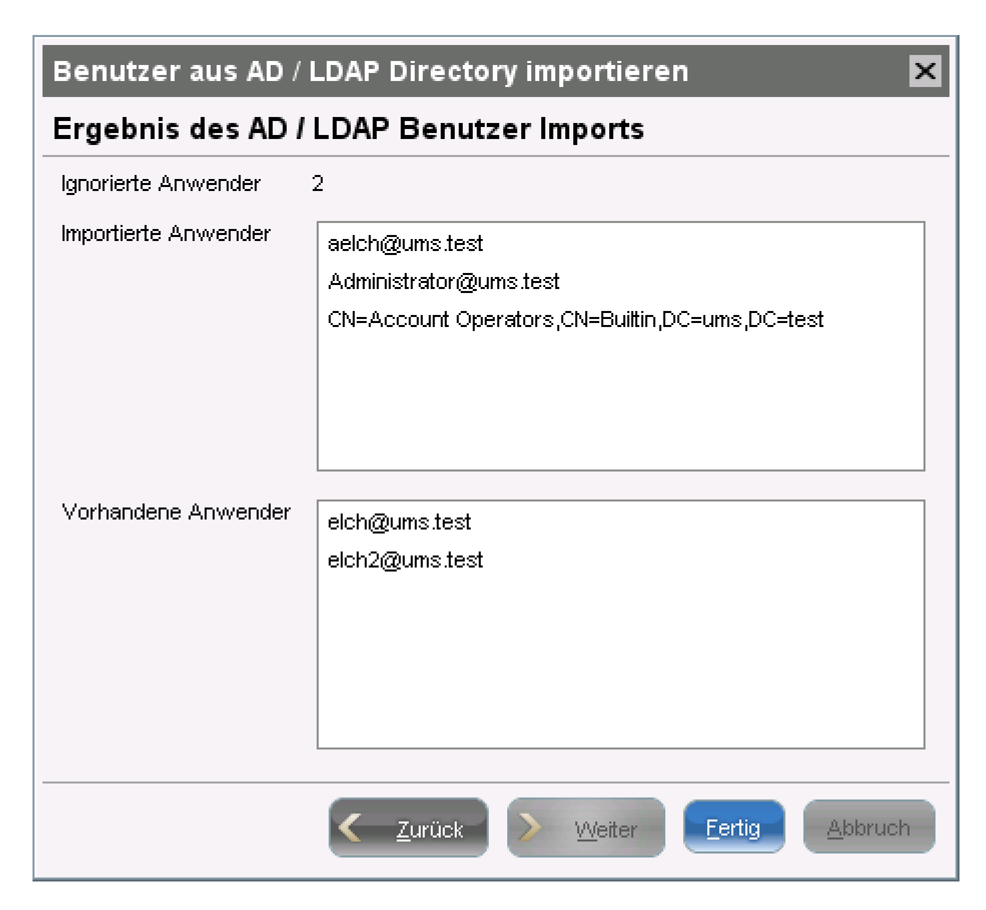


Abbildung 88: Ergebnis des Imports von AD-Benutzern

14. Administratorkonten und Zugriffsrechte

Für die Anmeldung an der UMS-Konsole können Sie UMS-Administratorkonten entweder aus einem angebundenen Active Directory importieren oder aber auch manuell erstellen, organisieren und entfernen.

An diesen Administratorkonten bzw. –gruppen hängen die Zugriffsrechte auf Objekte oder Aktionen innerhalb der IGEL UMS. Der Datenbankbenutzer, der bei der Installation oder Anlage der Datenquelle angelegt wurde, kann in seinen Rechten nicht beschränkt werden. Er hat immer alle Zugriffsrechte in der UMS.

14.1. Administratoren und Gruppen

➢ Klicken Sie **System→Administratorkonten**, um die IGEL UMS-Administratorkonten zu verwalten.

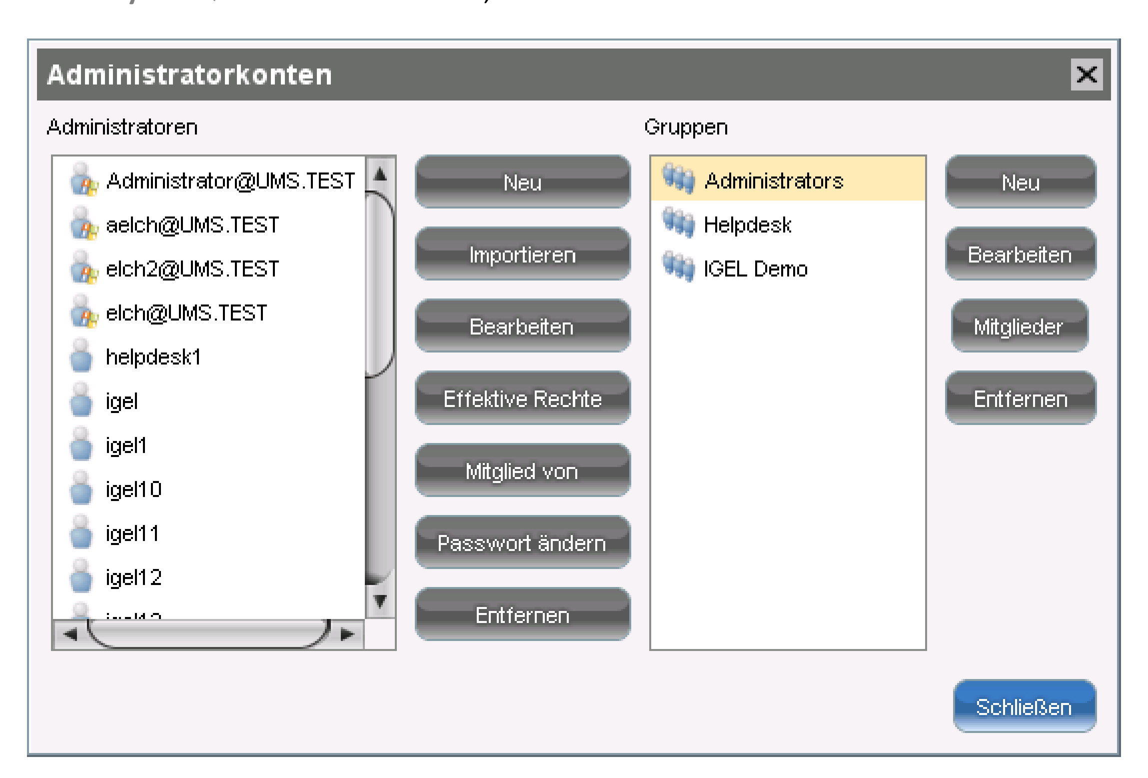


Abbildung 89: IGEL UMS-Administratorkonten

Alle vorhandenen Konten sind in der linken Spalte gelistet, die vorhandenen Gruppen in der rechten. Rechts der jeweiligen Spalte finden Sie die zugehörigen Schaltflächen wie **Neu**, **Bearbeiten**, **Entfernen**. Für Administratorkonten können Sie zudem das **Passwort ändern** und die Gruppenmitgliedschaft anzeigen. Auch für eine gewählte Gruppe lassen sich die darin enthaltenen **Mitglieder** anzeigen. Über **Effektive Rechte** haben Sie Einblick in die Rechte, die einem Benutzer direkt oder indirekt zugewiesen wurde, oder die ihm entzogenen wurden.

14.2. Zugriffsrechte

Berechtigungen in der IGEL UMS umfassen:

- allgemeine Rechte, die einem Administrator direkt über das Konto oder indirekt über die Gruppenzugehörigkeit zugewiesen bzw. verweigert werden können,
- Zugriffsrechte auf Objekte im Navigationsbaum,
- Aktionen in der UMS-Konsole.

Die indirekten Rechte, die ein Administrator über seine Gruppenzuweisung erhält, lassen sich für jeden Administrator der Gruppe weiter ändern. Dabei haben die direkt zugewiesenen Rechte Vorrang vor den indirekten.

Ein Administrator kann Mitglied mehrerer Gruppen sein und erhält die entsprechenden Rechte. Widersprechen sich Berechtigungen, so hat der Entzug einer Berechtigung Vorrang gegenüber der Gewährung. Wenn für eine Aktion oder ein Objekt aus einer Gruppe ein Verbot erlassen wird, übersteuert es beliebig viele Rechte aus anderen Gruppen.

Generell werden für Gruppen wie für Administratoren die gleichen Berechtigungseinstellungen vorgenommen. Im Folgenden werden die einzelnen Konfigurationsmöglichkeiten daher für Administratoren beschrieben, sie gelten aber ebenso für die Gruppenrechte.

14.2.1. Grundlegende Berechtigungen

In der nachfolgenden Tabelle sind die grundlegenden Zugriffsrechte gelistet, die zum Anlegen, Bearbeiten oder Löschen von Objekten benötigt werden. Ein Objekt ist z. B. ein Verzeichnis, Element des Navigationsbaums (Thin Clients, Profile…) oder auch Knoten im Administrationsbereich der Konsole, etwa administrative Aufgaben oder die AD-Anbindung.

Aktion	Betroffene Objekte	Durchsuchen	Lesen	Verschieben	Konf. Bearbeiten	Schreiben	Berechtigungen
Allgemein							
Objekt anzeigen	Baumelement (Profil, Thin Client…)		X				
	Verzeichnis	X					
Objekt anlegen	Zielverzeichnis					X	
Objekt löschen	Objekt					X	
	Quellverzeichnis					X	
Objekt bearbeiten	Objekt					X	
Objekt umbenennen	Objekt					X	
Konfiguration anzeigen	Thin Client, Profil		X				
Konfiguration bearbeiten	Thin Client				X		
	Profil					X	
Effektive Rechte anzeigen	Objekt		X				
	Verzeichnis	X					
Berechtigung ändern	Objekt, Verzeichnis						X
Import	Zielverzeichnis					X	

Abbildung 90: Grundlegende Zugriffsrechte

Beispiel 1:

Um die Konfiguration eines Thin Clients ändern zu können, benötigt ein Benutzer die **Durchsuchen-**Berechtigung auf den Verzeichnispfad des Thin Clients sowie das **Konfigurationsrecht** auf den Thin Clients selbst.

Beispiel 2:

Um ein zeitgesteuertes Backup der internen Datenbank konfigurieren zu können, benötigt der administrative Benutzer die Berechtigung für **Durchsuchen**, **Globale Konfiguration** und das **Schreibrecht** für administrative Aufgaben (Leserecht wird automatisch mit gesetzt).

14.2.2. Allgemeine Administratorenrechte

Die allgemeinen Administratorenrechte umfassen im Wesentlichen Aktionen im Menü der Konsole:

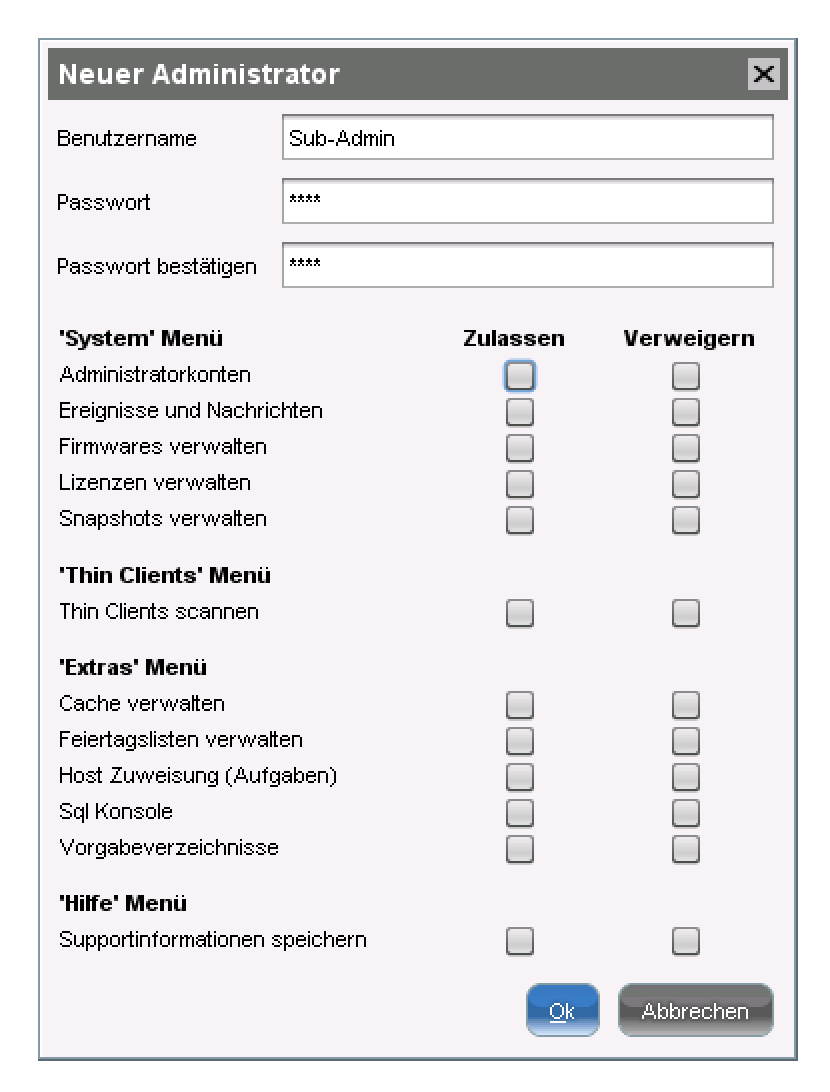


Abbildung 91: Menüberechtigungen des Administrators

Besondere Bedeutung kommt hierbei dem Punkt **Administratorkonten** zu. Dies ist die Berechtigungssteuerung selbst. Ein Administrator mit dieser Berechtigung kann für sich und andere Rechte gewähren und entziehen sowie neue Konten anlegen. Diese Berechtigung sollte nur Benutzern gewährt werden, die generell Zugriff auf alle Objekte und Aktionen in der UMS erhalten sollen.

Die Positionen im Einzelnen:

Administratorkonten	Die Berechtigungsverwaltung darf ausgeführt werden.
Ereignisse und Nachrichten	Einsicht in das Ereignis- und Nachrichten-Log ist zugelassen, wenn **Logging** aktiv ist.
Firmware verwalten	Firmwareversionen können importiert, exportiert und aus der Datenbank entfernt werden.
Lizenzen verwalten	IGEL-Firmwarelizenzen können an Thin Clients vergeben werden.
Snapshots verwalten	Snapshots für IGEL Thin Clients können am UMS-Server registriert und entfernt werden.
Thin Clients scannen	Es kann nach Thin Clients im Netzwerk gescannt werden, um diese z.B. am UMS-Server zu registrieren.
Cache verwalten	Der UMS-Servercache kann eingesehen und aktualisiert bzw. gelöscht werden.
Feiertagslisten verwalten	Feiertage können für die Planung von Aufgaben definiert werden.
Host Zuweisung	Geplante Aufgaben können verschiedenen Hosts zugewiesen werden.
SQL-Konsole	Die SQL-Konsole darf ausgeführt werden. **Vorsicht:** Die SQL-Konsole kann der Datenbank erheblichen Schaden zufügen!
Vorgabeverzeichnisse	Verzeichnisse und Regeln für die automatische Sortierung der Thin Clients dürfen angelegt und gelöscht werden.
Supportinformationen speichern	Datenbank- und Server-Logdateien können für Supportzwecke exportiert werden.

14.2.3. Objektbezogene Zugriffsrechte

Administratoren und Administratorengruppen können bestimmte Rechte an Objekten im Navigationsbaum zugewiesen werden. Diese Berechtigungen vererben sich „nach unten", also z. B. von einem Ordner auf die in diesem Ordner liegenden Thin Clients.

So gelangen Sie nach Auswahl eines Objekts zu den Berechtigungseinstellungen:

- über das Kontextmenü des Objekts
- oder über das Berechtigungssymbol in der Werkzeugleiste
- oder über den Menüpunkt **Bearbeiten→Berechtigungen**

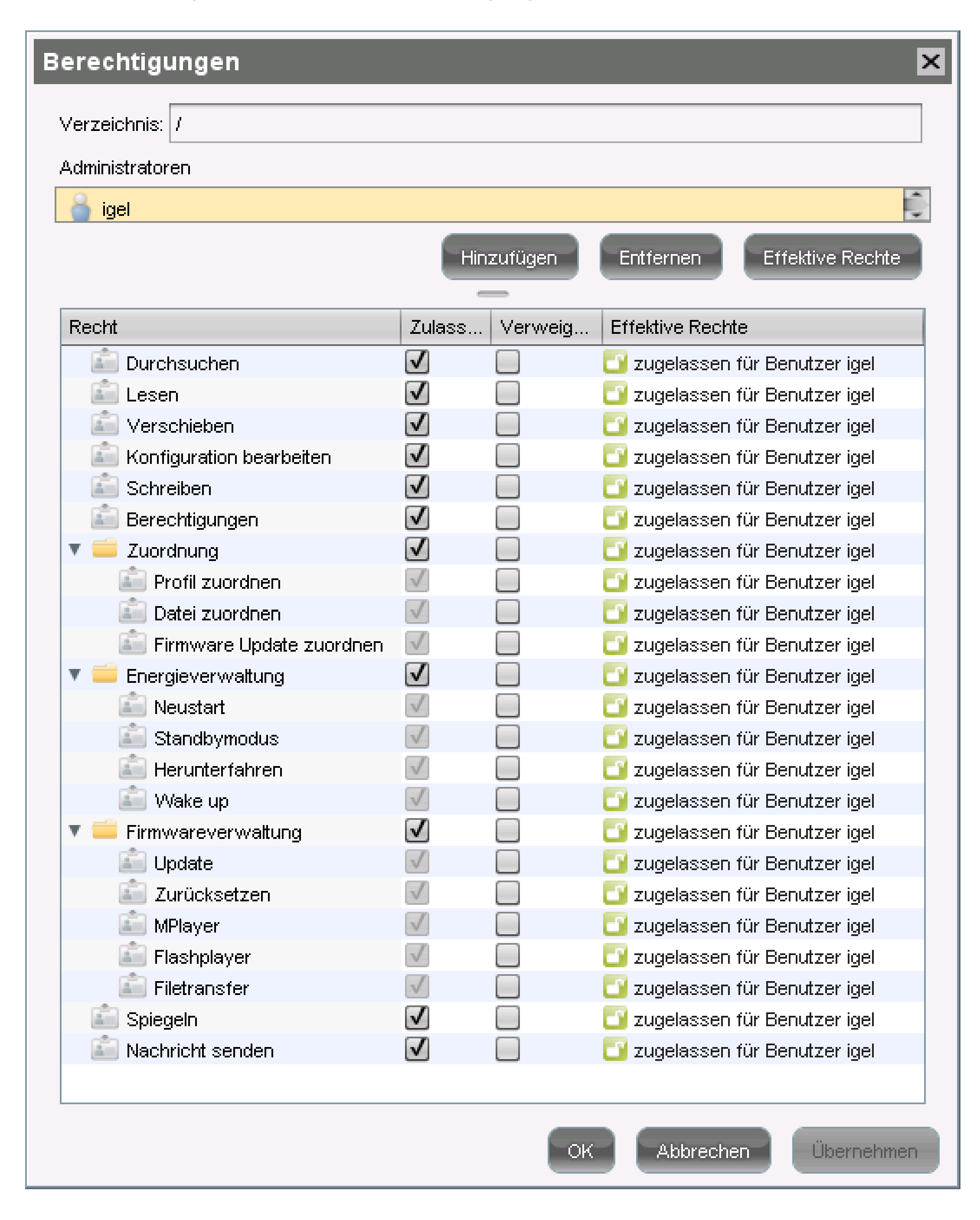


Abbildung 92: Objektberechtigungen

Obige Liste umfasst alle im UMS -Navigationsbaum verfügbaren objektbezogenen Berechtigungen. Je nach gewähltem Objekt steht davon nur eine Auswahl zur Verfügung. So lassen sich z. B. einer View weder Updates zuordnen, noch kann eine View heruntergefahren werden.

Zusammenhängende Berechtigungen werden automatisch zusammen gesetzt, können aber nachträglich manuell angepasst werden. Aktivierte Berechtigungen oder Verweigerungen auf Knoten betreffen alle Objekte im Knoten.

Die Übersicht zeigt für einen ausgewählten Administrator dessen Rechte am Objekt. Details erhält man über **Effektive Rechte**. Hier werden auch die Regeln der Rechteermittlung angezeigt, z. B. ob eine Berechtigung direkt vergeben wurde oder ob sie über eine Gruppe oder eine Vererbung in der Baumstruktur zugewiesen ist.

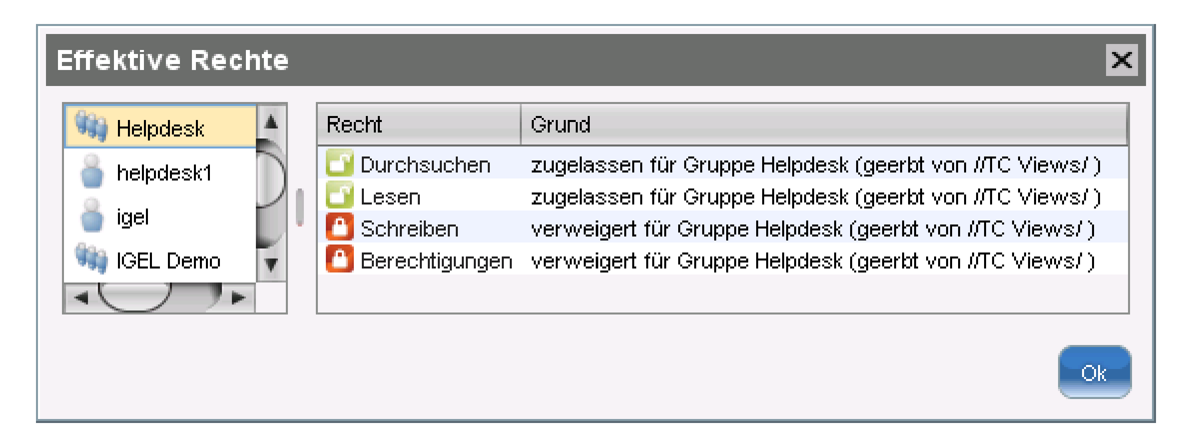


Abbildung 93: Effektive Rechte

Verfügbare Rechte

Allgemein	**Durchsuchen**	Sichtbarkeit des Objekts im Navigationsbaum (Pfad bis zum Objekt muss ebenfalls erlaubt werden!)
	Lesen	Leserecht auf Ordnerinhalte bzw. Objekteigenschaften
	Verschieben	Thin Clients dürfen ohne Schreibrecht verschoben werden.
	Konfiguration bearbeiten	Schreibrecht für die Konfiguration eines Thin Clients (TC-Setup)
	Schreiben	Schreibrecht auf Ordner bzw. Objekteigenschaften (nicht TC-Setup)
	Berechtigungen	Die Berechtigungseinstellungen des Objekts dürfen geändert werden.
	Spiegeln	VNC-Zugriff auf den Thin Client
	Nachricht senden	Nachrichtenfunktion des Thin Clients
Zuordnung	**Profil zuordnen**	Dem Objekt darf ein Profil zugeordnet werden.
	Datei zuordnen	Dem Objekt darf eine Datei zugeordnet werden.
	Update zuordnen	Dem Objekt darf ein Firmwareupdate zugeordnet werden.
Energie	**Neustart**	Den Thin Client neu starten.
	Ruhezustand	Den Thin Client in den Ruhezustand versetzen.
	Herunterfahren	Den Thin Client herunterfahren.
	Wake up	Den Thin Client per Wake-on-LAN aufwecken.

Firmware	**Update**	Das Firmwareupdate darf durchgeführt werden.
	Zurücksetzen	Die Firmware auf Werkseinstellungen zurücksetzen.
	Media Player	Codeclizenzen für den Media Player herunterladen (IGEL LX 3.x).
	Flash Player	Lizenz für den Adobe Flash Player herunterladen.
	Filetransfer	Eine zugewiesene Datei darf zum Thin Client übertragen werden.

14.2.4. Zugriffsrechte im Administrationsbereich

Im Administrationsbereich der Konsole können Sie die allgemeinen Rechte **Durchsuchen**, **Lesen**, **Schreiben**, **Berechtigungen** für Administratorkonten vergeben bzw. verweigern. Berechtigungen sollten nur an Benutzer vergeben werden, die tatsächlich administrative Aufgaben an der UMS ausführen sollen.

15. Benutzerprotokolle

Das Protokollsystem wird von der UMS und den registrierten Thin Clients verwendet, um alle Datenbankänderungen aufzuzeichnen. Nur erfolgreiche Aktionen werden protokolliert. Fehler finden Sie in der Protokolldatei des UMS GUI-Servers nicht.

Das Protokollsystem ist in zwei Bereiche unterteilt:

Messages (Nachrichten): Von einem Benutzer gestartete Aktionen.

Events (Ereignisse): Von einem Thin Client gestartete Aktionen.

15.1. Administration

Die Administrationseinstellungen für den Protokollierungsvorgang werden im IGEL UMS-Administrator unter **Einstellungen→Logging** konfiguriert.

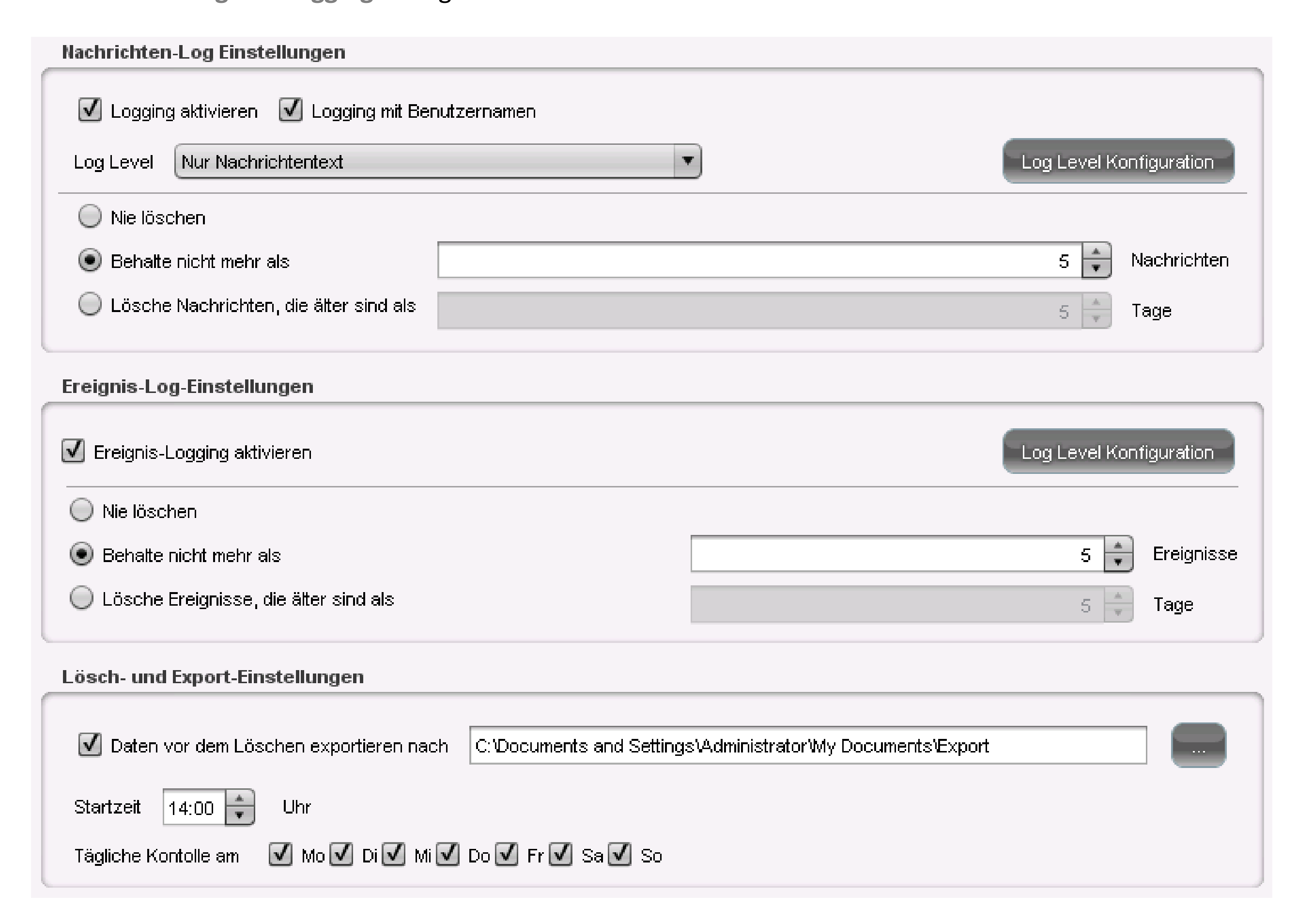


Abbildung 94: Administrationseinstellungen vornehmen

- **Nachrichten** können entweder mit oder ohne Details protokolliert werden.

  Für **Ereignisse** gibt es keine Details.

- Alte Nachrichten können automatisch aus der Liste gelöscht werden. Sie können festlegen, wie lange oder wie viele Nachrichten aufbewahrt werden. Sie können ein Exportverfahren einrichten, um Nachrichten zu sichern, bevor sie automatisch gelöscht werden.
- Mit den **Log Level**-Schaltflächen aktivieren Sie die Protokollierung für ausgewählte Befehle. Standardmäßig ist die Protokollierung für alle möglichen Befehle ausgewählt.

Mit **Anwenden** werden die Einstellungen gespeichert und für den RMGuiServer-Dienst angewendet.

15.2. Dialogfenster Logging

Meldungen zu **Nachrichten** und **Ereignisse** lassen sich in der Konsole folgendermaßen anzeigen:

- über das Menü **System→Logging**
- über **Logging** im Kontextmenü der Verzeichnisse und Objekte im Navigationsbaum

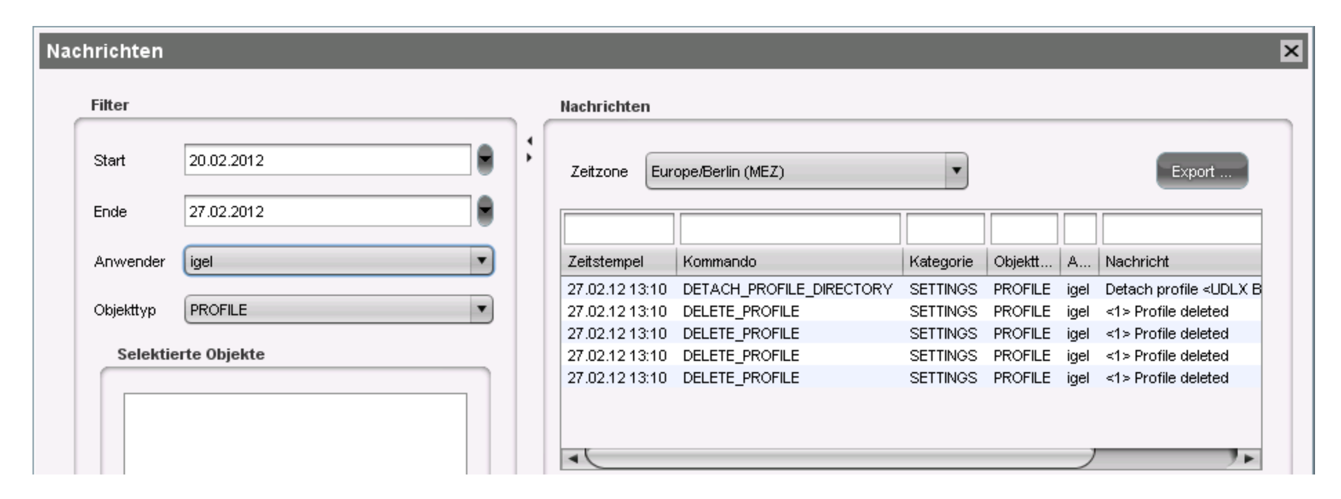


Abbildung 95: Nachrichten-Logging

15.2.1. Filter einstellen

So stellen Sie einen Filter ein:

1. Geben Sie Im Fensterbereich **Filter** Kriterien an, um selektive Nachrichten aus der Datenbank zu laden.

   Alle Filterfelder werden mit dem Operator **AND** kombiniert.
   Nur wenn die Mehrfachauswahl für ein Filterfeld möglich ist, werden diese Werte mit dem Operator **OR** verbunden, z. B. wenn mehrere Thin Clients ausgewählt werden.

2. Klicken Sie auf **Filter anwenden** um die neuen Einstellungen zu aktivieren.

   Die Protokollnachrichten oder -ereignisse werden aus der Datenbank entsprechend den Filtereinstellungen neu geladen.

> **Nachrichten/Ereignisse** können mit **Export** in HTML-, XML- und CSV-Dateien exportiert werden.

Filter für Ereignisse einstellen

So stellen Sie den Filter für Ereignisse ein:

1. Geben Sie das Kommando an, wenn es Ihnen bekannt ist.
2. Geben Sie die MAC-Adresse des Thin Clients an, für den die Ereignisse angezeigt werden sollen.

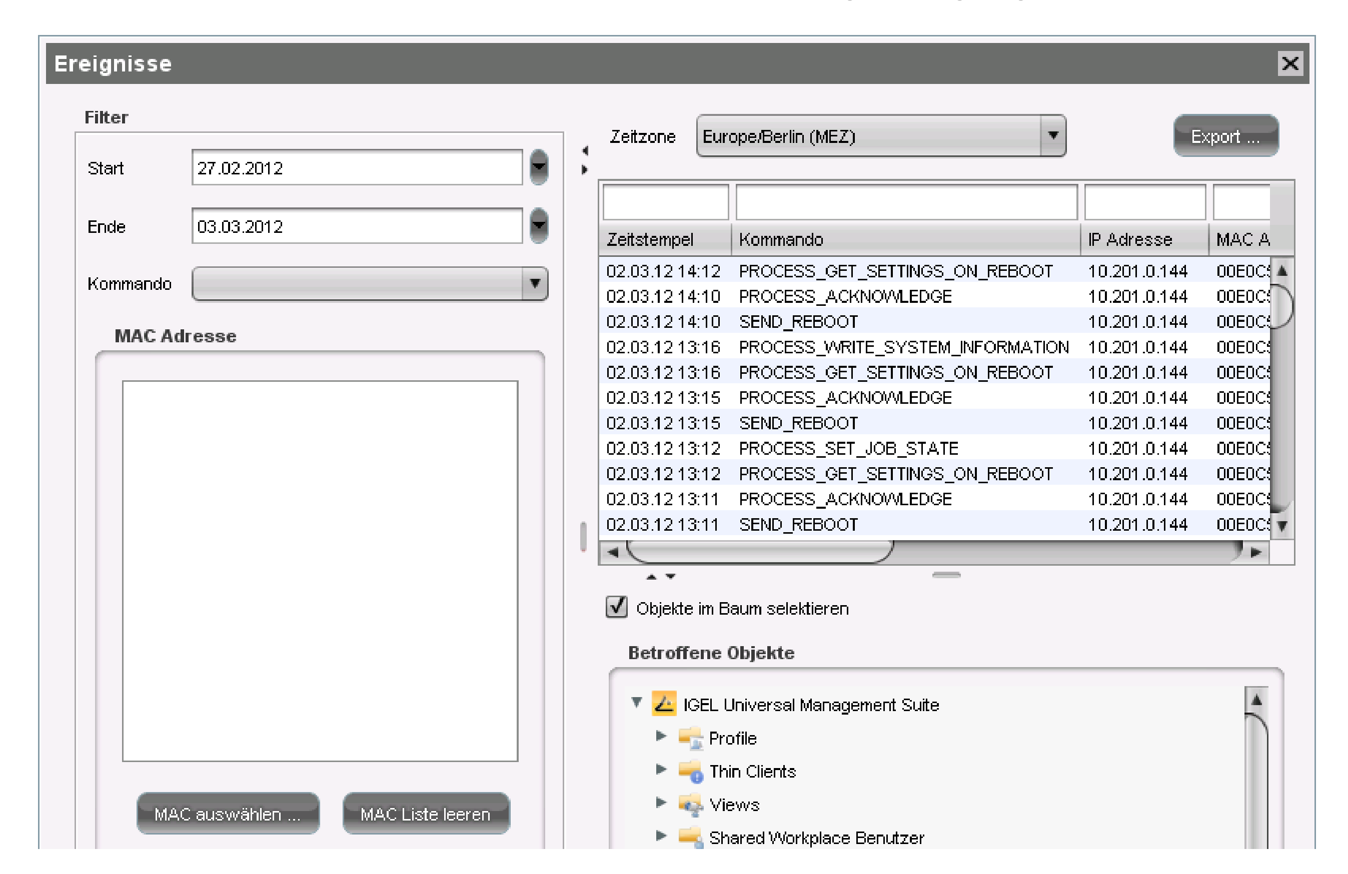


Abbildung 96: Ereignis Logging

Filter für Nachrichten

Anwender	Wählen Sie den Namen des UMS-Administrators aus, der für die Nachricht zuständig ist. Wenn dieses Feld leer bleibt, werden die Nachrichten aller Benutzer angezeigt.
Objekttyp	Geben Sie ein Objekt an, für das Sie die Nachrichten anzeigen lassen möchten. Wenn dieses Feld leer bleibt, werden die Nachrichten für alle Objekttypen angezeigt.
Kategorie	Jeder Befehl gehört einer Kategorie an, z. B. Sicherheit, Einstellungen und Objekte.
Kommando	Wenn ein Kommando bekannt ist, können Sie dieses selbst angeben.
Zeitzone	Sie können die Zeitzone angeben, mit der die Protokollzeit der Nachrichten angezeigt wird.

Filter für Kategorien einstellen

➢ Wählen Sie für die Anpassung des Filters die Option **Kategorie**, wenn Sie alle Nachrichten für eine bestimmte Kategorie (wie z. B. zu Firmware Updates) auswählen möchten.

  Alle Kommandos dieser Kategorie wie **Firmware Update Löschen** oder **Firmware Update zuweisen** werden für die Ermittlung der Nachrichten oder Ereignisse ausgewertet.

Anmerkungen

Der Schnellfilter gilt nicht für die Exportaktion.

Einer der wichtigsten Befehle ist der Befehl `GET_SETTINGS_ON_REBOOT`. Über den Zeitstempel dieses Befehls erhalten Sie die letzte Startzeit auf dem Thin Client. Diese kann verwendet werden, um ein neues **BOOTTIME-**View-Kriterium zu definieren. Mit diesem Kriterium können Sie alle Thin Clients ganz einfach ermitteln, die nach einem bestimmten Datum noch nicht gestartet worden sind.

> Die Administrationseinstellungen für die Menge der Nachrichten und - noch wichtiger - für die Ereignisse sollten mit großer Sorgfalt gehandhabt werden. Je höher diese Werte sind, umso mehr Platz wird für den Tablespace in der Datenbank benötigt. Wenn Sie die Protokollierung aktivieren, sollten Sie Ihre Datenbank genau beobachten, bis Sie sich sicher sind, dass in der Datenbank ausreichend Platz für die Nachrichten und/oder Ereignisse verfügbar ist.

16. Logdateien und Support

Falls Sie Probleme mit der IGEL UMS haben und Ihren Serviceanbieter kontaktieren, können Sie verschiedene Logdateien der UMS mitliefern. Sie können diese Logs leicht als ZIP-Archiv generieren, wählen Sie dazu **Hilfe→Support Information speichern**.

Bei Fragen rund um das IGEL-Produkt, wenden Sie sich bitte zunächst an den für Sie zuständigen Vertriebspartner, sofern Sie bereits IGEL-Kunde sind.

Wenn Sie zur Zeit IGEL-Produkte testen, oder falls Sie von Ihrem Vertriebspartner die gewünschte Hilfe nicht bekommen können, füllen Sie bitte nach dem Einloggen auf der Seite `http://www.igel.com/de/mitgliederbereich/anmelden-abmelden.html` das Supportformular aus.

Wir werden Sie umgehend unterstützen. Sie erleichtern die Arbeit unserer Supportmitarbeiter, wenn Sie uns möglichst alle verfügbaren Informationen zukommen lassen. Bitte beachten Sie hierzu auch unsere Hinweise zu Support- und Serviceauskünften.

Besuchen Sie auch unsere IGEL Knowledge Base http://edocs.igel.com/. Dort finden Sie neben den Benutzerhandbüchern auch die Support-FAQ und ergänzende Dokumentation in Form von Best Practice oder Howto.

17. Optionale Erweiterungen (HA und UCB)

In diesem Anhang finden Sie umfassende Informationen zu den optionalen Zusatzfunktionen der IGEL UMS High Availability Extension und des IGEL Universal Customization Builder.

17.1. IGEL UMS High Availability (HA)

Die High Availability Extension ist ein optional nutzbarer Bestandteil der IGEL UMS ab Version 4.0. Sie adressiert große Thin Client-Umgebungen, in denen neue Einstellungen simultan an mehrere hundert Thin Clients ausgerollt werden müssen, oder in denen der ausfallsichere Rollout neuer Einstellungen geschäftskritisch ist. Die technische Umsetzung basiert auf einem Verbund mehrerer UMS-Managementserver.

Ein vorgeschalteter UMS-Load Balancer übernimmt die Lastverteilung und stellt somit sicher, dass jeder Thin Client jederzeit neue Einstellungen erhalten kann. Auch wenn sich zum Arbeitsbeginn mehrere tausend Geräte gleichzeitig am UMS-Server anmelden und nach neuen Konfigurationsprofilen oder Firmwareupdates suchen. Hinsichtlich maximaler Prozesssicherheit und Hochverfügbarkeit empfiehlt IGEL, auch den UMS-Load Balancer sowie die UMS-Datenbank redundant auszulegen.

Die High Availability Extension wird in Paketen zu 50 Lizenzen angeboten und erfordert die vollständige Lizenzierung aller gemanagten Thin Clients. Jede Version der IGEL UMS 4 enthält fünf Testlizenzen, dank derer sich die Funktion kostenlos und ohne Registrierung evaluieren lässt.

Beachten Sie auch unser Best Practice *New Installation of an HA Network* *http://edocs.igel.com/index.htm#10200454.htm*.

17.1.1. Konfigurationsoptionen

Prinzipiell können beliebig viele UMS-Server und Load Balancer in einem HA-Netzwerk miteinander verbunden werden. Zwei grundsätzliche Szenarien für typische Anwendungsfälle sollen aber detaillierter beschrieben werden:

- die einfache Hochverfügbarkeit, um z. B. für eine relativ geringe Zahl von Thin Clients die Verfügbarkeit von Benutzerprofilen (Shared Workplace) sicherzustellen
- die Lastverteilung (Netzwerk mit vielen Thin Clients)

UMS-Server und Load Balancer müssen IP-technisch im gleichen Netz stehen, ohne NAT oder Proxys, welche die Kommunikation der Komponenten beeinflussen.

Einfache Hochverfügbarkeit

Damit Benutzer, die sich am Thin Client mit ihrem AD-Benutzerkonto anmelden, auch sicher das ihnen zugewiesene Profil erhalten (Thin Client Firmware mit Shared Workplace Feature Set), ist eine Redundanz sowohl des Servers als auch des Load Balancers notwendig. Die Datenbank ist im Idealfall als Cluster ausgelegt, um diese Fehlerquelle zu minimieren.

Sind nur relativ wenige Thin Clients im Netzwerk zu verwalten, ist die Lastverteilung zu vernachlässigen. Es reichen zwei Serversysteme aus, die sich wechselseitig ersetzen können. Auf jedem der beiden Systeme wird die komplette HA-Erweiterung installiert, also jeweils ein UMS-Server und ein Load Balancer.

Das System besteht somit aus:

- zwei Load Balancern, die für Thin-Client-Anfragen bereitstehen
- zwei UMS-Servern, die für jeden der beiden Load Balancer erreichbar sind
- einer ausfallsicheren Datenbank, z. B. einem Microsoft SQL Server-Cluster

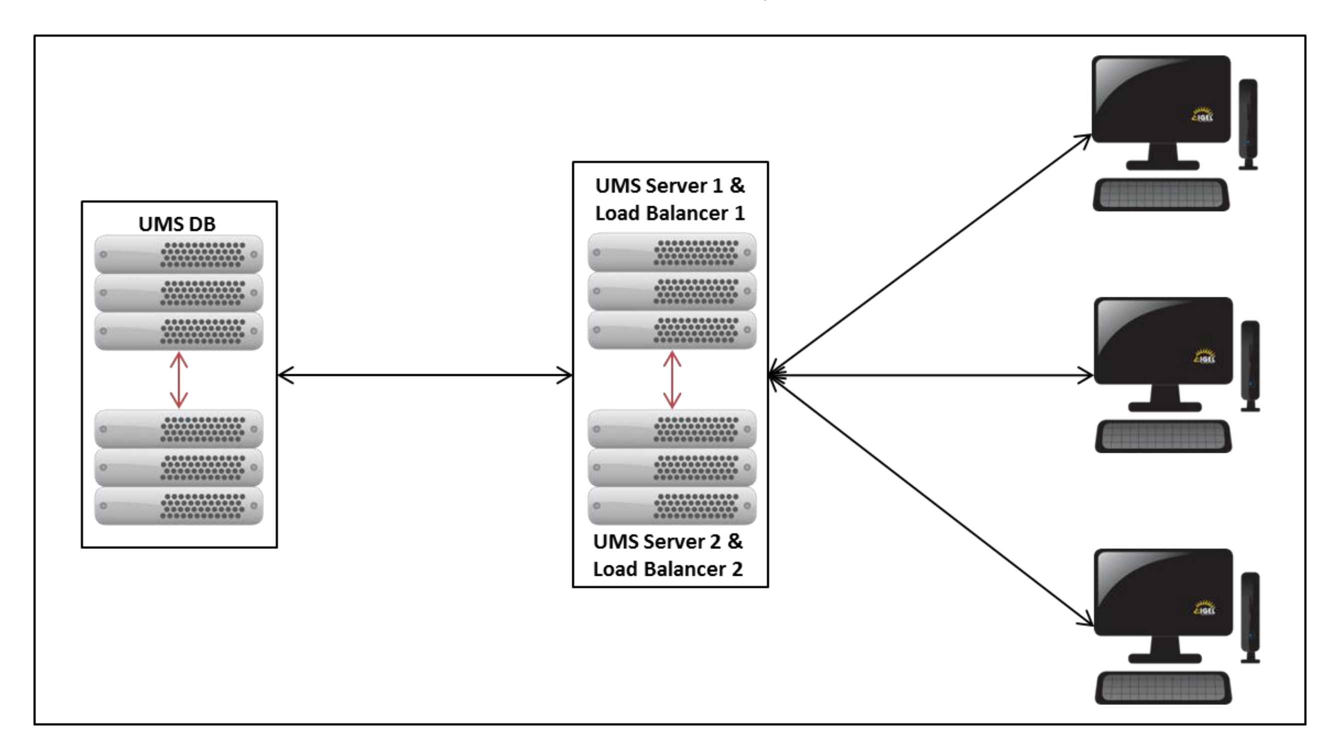


Abbildung 97: Einfache Hochverfügbarkeitslösung

Jedes der beiden Systeme kann auch allein die Aufgaben als UMS-Server erfüllen. Sind beide Systeme gleichzeitig aktiv, ergibt sich eine gewisse Lastverteilung, die aber vergleichsweise gering ausfällt. Denn neben dem eigentlichen UMS-Server erzeugt der Load Balancer zusätzlich Last. Für die Verwaltung vieler Thin Clients sollten daher UMS-Server und Load Balancer auf getrennten Systemen betrieben werden, s.u. *Lastverteilung* (Seite 145).

Hochverfügbarkeit und Lastverteilung

Die kleinste Konfiguration mit echter Lastverteilung umfasst vier bis fünf getrennte Serversysteme:

- zwei Load Balancer,
- zwei bis drei UMS-Server,
- eine leistungsfähige und ausfallsichere Datenbank (Cluster).

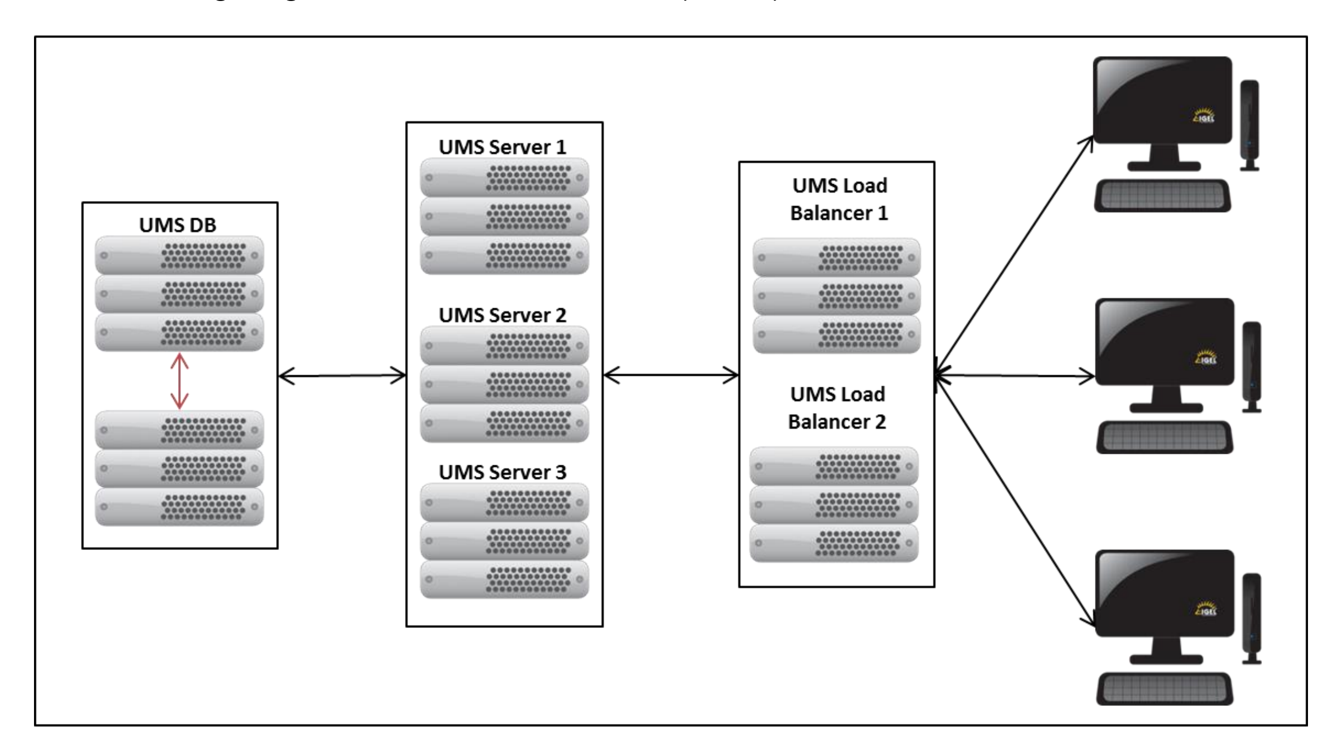


Abbildung 98: Hochverfügbarkeit und Lastverteilung

Anfragen von den Thin Clients können von beiden Load Balancern an die UMS-Server weitergereicht werden. Sollte einer der Load Balancer ausfallen, ist der andere weiterhin erreichbar und übernimmt die Kommunikation allein. Daher sind auch nicht mehr als drei UMS-Server in dieser Konfiguration vorgesehen. Eine größere Anzahl von Servern könnte einen einzigen Load Balancer überlasten und dieser würde selbst den Flaschenhals bilden. Für sehr große Installationen mit mehr als drei UMS-Servern, sollte auch die Zahl der Load Balancer entsprechend erhöht werden. Dabei gilt die Faustregel, dass ein Load Balancer allein bis zu drei Server bedienen kann.

Faustregel für eine sinnvolle Lastverteilung: Pro 2.000 verwaltete Thin Clients ein Server und pro 5.000 Thin Clients ein Load Balancer.

17.1.2. HA_Installation

Hier erfahren Sie mehr über:

- *Installationsvoraussetzungen* (Seite 147)
- *Neuinstallation* (Seite 147)
- *Anbindung externer Datenbanksysteme* (Seite 17)
- *Lizenzierung der High-Availability-Erweiterung* (Seite 152)

Installationsvoraussetzungen

Um ein IGEL-UMS-High-Availability-Netzwerk installieren zu können, müssen folgende Mindestanforderungen an Hard- und Software erfüllt sein.

> **Warnung:** UMS-Server darf nicht auf einem Domain-Controller-System installiert werden. Die manuelle Änderung des Java Runtime Environment auf dem UMS-Server wird nicht empfohlen. Der Betrieb zusätzlicher Apache Tomcat-Webserver zusammen mit dem UMS-Server wird ebenfalls nicht empfohlen.

Installation UMS-Server - auch einzelne HA-Netzwerkkomponenten

- Betriebssystem: Microsoft Windows Server 2003/2008 R2 und neuer
- Mind. 512-MB-RAM verfügbar, 1024 MB empfohlen
- Mind. 400 MB freier HDD-Speicher (Zzgl. Datenbanksystem)

> Auf Windows Server 2008 R2 (und neuer) stellen Sie bitte vor der UMS-Installation sicher, dass der 32-bit-Kompatibilitätsmodus aktiv ist.

Installation UMS-Konsole

- Mind. 256-MB-RAM, 512 MB empfohlen
- Mind. 50-MB-HDD-Speicher
- Java Web Start-Konsole: Java 1.8.0_40 oder neuer erforderlich
- Die unterstützten Betriebssysteme entnehmen Sie bitte dem UMS-Datenblatt auf der IGEL-Webseite.

Datenbanksysteme (DBMS)

Die unterstützten Datenbanksysteme finden Sie im UMS-Datenblatt auf der IGEL-Webseite. Die Installations- und Betriebsvoraussetzungen für die Datenbank finden Sie in der Dokumentation des jeweiligen DBMS.

UMS-Server und Load Balancer für Hochverfügbarkeit (*High Availabilty* (Seite 143), HA) müssen IP-technisch im gleichen Netz stehen, ohne NAT oder Proxys, welche die Kommunikation der Komponenten beeinflussen.

Die interne Datenbank (Embedded-DB) kann **nicht** für ein HA -Netzwerk verwendet werden. Für eine reine Testinstallation mit nur einem einzigen Server für UMS-Server und Load Balancer können Sie auch die Embedded-Datenbank verwenden. Ein echtes HA-Netzwerk lässt sich damit jedoch nicht aufbauen.

Installation der einfachen Hochverfügbarkeitslösung

Für die Nutzung der High-Availability-Erweiterung wählen Sie bitte die Installation der HA-Netzwerkkomponenten (UMS-Server und UMS-Load-Balancer).

In diesem Beispiel wird die Installation der einfachen Hochverfügbarkeitslösung beschrieben. Auf jedem der Server werden somit UMS-Server und Load Balancer installiert. Bei abweichenden Installationen wählen Sie die entsprechenden Komponenten einzeln aus.

Erster Server des HA-Netzwerks

So installieren Sie den ersten Server des HA-Netzwerks:

1. Laden Sie sich die aktuelle Version der IGEL Universal Management Suite vom IGEL-Downloadserver herunter.
2. Starten Sie den Installer durch Ausführen der EXE-Datei.

   > Sie benötigen Administrationsrechte auf dem Rechner, um IGEL UMS installieren zu können.

3. Schließen Sie andere Anwendungen und bestätigen Sie dies.
4. Lesen und bestätigen Sie die Lizenzvereinbarung.
5. Lesen Sie die Erläuterung des Installationsprozesses.
6. Wählen Sie einen Pfad für die Installation.
7. Wählen Sie den Installationsumfang (hier: HA-Netzwerk mit Server und Load Balancer).
8. Bestätigen Sie die Meldung zur Lizenzierung der HA-Erweiterung.
9. Aktivieren Sie die Option zur Erstellung eines IGEL-Network-Tokens.
10. Geben Sie einen Speicherort für das Token an.
11. Wählen Sie einen Namen für den Eintrag im Windows-Startmenü.
12. Lesen Sie die Zusammenfassung und starten Sie den Prozess.
13. Schließen Sie das Programm nach Abschluss der Installation.

    Haben Sie die Installation eines UMS-HA-Netzwerks gewählt, läuft nun der IGEL Universal Management Suite-Server sowie ein Load Balancer auf diesem Rechner.

Der Windows-Installer erstellt Einträge im Windows-Softwareverzeichnis und im Startmenü. Ein Icon zum Start der UMS-Konsole wird auf dem Desktop abgelegt.

> Warnung: Das IGEL-Netzwerk-Token wird für die Installation weiterer Server benötigt. Sichern Sie dieses gut.

Weitere Server

Die Installation weiterer UMS-Server läuft analog zum ersten Server. Allerdings legen Sie hier kein neues Netzwerktoken an. Stattdessen wählen Sie das zuvor am ersten Server erstellte Token bei der Installation aus, damit sich neue Server in das HA-Netzwerk integrieren. Legen Sie dieses Token also vor der Installation auf einem für den Server erreichbaren Speicher ab (z. B. im Netzwerk oder auf einem portablen Speicher wie USB-Stick).

Zudem muss nach der Installation eines weiteren UMS Servers die Verbindung mit der selben UMS Datenbank hergestellt werden, die auch vom ersten Server verwendet wird. Das UMS HA-Netzwerk funktioniert nur, wenn alle Server mit der gleichen Datenbank verbunden sind.

So installieren Sie weitere Server:

1. Laden Sie sich die aktuelle Version der IGEL Universal Management Suite vom IGEL-Downloadserver herunter.
2. Starten Sie den Installer durch Ausführen der EXE-Datei.

   > Sie benötigen Administrationsrechte auf dem Rechner, um IGEL UMS installieren zu können.

3. Schließen Sie andere Anwendungen und bestätigen Sie dies.
4. Lesen und bestätigen Sie die Lizenzvereinbarung.
5. Lesen Sie die Erläuterung des Installationsprozesses.
6. Wählen Sie einen Pfad für die Installation.
7. Wählen Sie den Installationsumfang (hier: HA-Netzwerk mit Server und Load Balancer).
8. Bestätigen Sie die Meldung zur Lizenzierung der HA-Erweiterung.
9. Deaktivieren Sie die Option zur Erstellung eines IGEL-Network-Tokens.
10. Wählen Sie das zu verwendende Token aus.
11. Optional: Laden Sie eine `tc.keystore` Datei.
12. Wählen Sie einen Namen für den Eintrag im Windows-Startmenü.
13. Lesen Sie die Zusammenfassung und starten Sie den Prozess.
14. Schließen Sie das Programm nach Abschluss der Installation.

Bei weiteren HA-Servern müssen Sie diedie Datenquelle folgendermaßen eintragen und aktivieren:

1. Starten die den UMS Administrator:
2. Erstellen Sie eine Datenquelle, und tragen Sie die identischen Parameter ein, die auch von Server 1 verwendet werden.
3. Aktivieren Sie die neue Datenquelle.
4. Beenden Sie den UMS Administrator.

Haben Sie die Installation eines UMS-HA-Netzwerks gewählt, läuft nun der IGEL Universal Management Suite-Server sowie ein Load Balancer auf diesem Rechner.

Der Windows-Installer erstellt Einträge im Windows-Softwareverzeichnis und im Startmenü. Ein Icon zum Start der UMS-Konsole wird auf dem Desktop abgelegt.

> Warnung: Das IGEL-Netzwerk-Token wird für die Installation weiterer Server benötigt. Sichern Sie dieses gut.

Installation einzelner HA-Netzwerkkomponenten

Die getrennte Installation von UMS-HA-Netzwerkkomponenten läuft vergleichbar ab, auch hier ist es so, dass bei Installation der ersten Komponenten (Server oder Load Balancer) ein Netzwerktoken erstellt und für die Installation weiterer Komponenten verwendet wird.

Wird ein UMS-Server einzeln installiert, so sind auf dem System neben den Serverdiensten die Anwendungen UMS-Konsole und UMS-Administrator zur Verwaltung der Installation verfügbar. Nach dem

Konfigurieren und Aktivieren der HA-Netzwerkdatenbank über den UMS Administrator ist der Server im HA-Netzwerk verfügbar.

Bei Installation eines einzelnen Load Balancers wird nur dessen Service installiert und automatisch gestartet. Im Windows-Startmenü wird lediglich die Option zur Deinstallation der Universal Management Suite angelegt. Am Load Balancer ist keine Konfiguration nötig. Er verbindet sich beim Starten selbstständig mit dem HA-Netzwerk.

Anbindung externer Datenbanksysteme

Die unterstützten Datenbanksysteme finden Sie im Datenblatt der IGEL UMS bzw. der HA-Erweiterung auf der IGEL-Webseite. Die Installations- und Betriebsvoraussetzungen für die Datenbank finden Sie im Administrationshandbuch des jeweiligen DBMS.

- Konfigurieren Sie die Datenbank im jeweiligen Verwaltungsprogramm des DBMS.

Die Erstellung der Datenquelle und Anbindung der UMS an die Datenbank konfigurieren Sie im UMS-Administrator.

> Alle UMS-Server müssen mit der selben Datenbank arbeiten.

Oracle

So binden Sie Oracle an:

1. Erstellen Sie einen neuen Datenbankbenutzer mit `Ressource`–Berechtigung.
2. Legen Sie im UMS-Administrator eine neue Datenquelle vom Typ Oracle an.

> Einige Oracle-Versionen legen die Rolle `Ressource` ohne `CREATE VIEW`–Berechtigung an, stellen Sie sicher, dass diese Berechtigung in der Rolle gesetzt ist.

Microsoft SQL Server

So binden Sie Microsoft SQL Server an:

1. Öffnen Sie die SQL-Konsole des SQL-Servers über **New Query**.
2. Verwenden Sie das folgende Skript als Vorlage, passen Sie es an und führen Sie es aus.

> Um Probleme bei der Aktivierung der Datenquelle zu vermeiden stellen Sie bitte sicher, dass `LOGIN`, `USER` und `SCHEMA` gleich benannt sind.

```
CREATE DATABASE rmdb
GO
USE rmdb
GO
CREATE LOGIN igelums with PASSWORD = 'setyourpasswordhere',
DEFAULT_DATABASE=rmdb
GO
CREATE USER igelums with DEFAULT_SCHEMA = igelums
GO
CREATE SCHEMA igelums AUTHORIZATION igelums GRANT CONTROL to igelums
GO
```

3. Legen Sie im UMS-Administrator eine neue Datenquelle vom Typ `SQL Server` an.
4. Stellen Sie sicher, dass der **Serverport** des SQL-Servers in der Datenquelle korrekt konfiguriert ist, der Standardwert ist `1433`.

   Der Microsoft-SQL-Server sollte **Windows- und SQL-Authentifizierung** zulassen.

PostgreSQL

So binden Sie PostgreSQL an:

Setzen Sie bei der Installation einer neuen Instanz der PostgreSQL-Datenbank folgende Parameter:

1. Installieren Sie das Datenbankcluster mit `UTF-8` **Kodierung.**
2. Akzeptieren Sie Verbindungen aller **Adressen**, nicht nur `localhost`.
3. Aktivieren Sie **Procedural Language** `PL/pgsql` in der Defaultdatenbank.

   Weitere Informationen zur Installation der PostgreSQL-Datenbank finden Sie unter http://www.postgresql.org.

Führen Sie nach der Installation folgende Konfigurationsschritte aus:

1. Ändern Sie die Serverparameter: In der Datei `postgresql.conf` muss der Parameter `listen_addresses` den Hostnamen des IGEL UMS-Server enthalten **ODER** `'*',` um Verbindungen zu jedem Host zuzulassen.
2. Legen Sie in der Datei `pg_hba.conf` einen Parameter `host` an, um dem UMS-Server die Berechtigung für das Log-in mit den dort definierten Benutzerdaten zu geben.

   > Ist der IGEL UMS-Server auf derselben Maschine wie PostgreSQL-Server installiert, so sind keine Änderungen an diesen Dateien notwendig.

3. Starten Sie das Administrationstool pgAdmin.
4. Erstellen Sie eine neue Log-in-Rolle mit dem Namen `rmlogin`.
5. Erstellen Sie eine neue Datenbank mit

   name = `rmdb`
   owner = `rmlogin`
   encoding = `UTF-8`

6. Legen Sie ein neues Schema innerhalb der Datenbank rmdb an mit

   name = `rmlogin`

7. Prüfen Sie ob die Sprache plpgsql in der Datenbank rmdb besteht.

   Falls nicht, legen Sie diese an.

8. Legen Sie im **UMS-Administrator** eine neue Datenquelle vom Typ `PostgreSQL` an mit dem Hostnamen des PostgreSQL-Servers und dem korrekten Serverport (Vorgabe ist `5432`), Benutzer `rmlogin` und Datenbank `rmdb`.

Apache Derby

So binden Sie Apache Derby an:

Wie für die anderen externen Datenbanken empfehlen wir auch hier für die Verwendung durch IGEL UMS eine neue Datenbankinstanz anzulegen.

Führen Sie die folgenden Schritte aus, um eine neue Datenbankinstanz anzulegen und definieren Sie diese als Datenquelle im **UMS-Administrator**:

1. Aktivieren Sie zur Sicherheit **User Authentication** in der Derby-DB.
2. Starten Sie das ij Utility (in `[derby-installation-dir]/bin`).
3. Führen Sie folgendes Kommando aus, um die Instanz rmdb anzulegen:
   ```
   connect
   'jdbc:derby:rmdb;user=dbm;password=dbmpw;create=true';
   ```
4. Definieren Sie den UMS-Datenbankbenutzer `rmlogin` mit Passwort `rmpassword`
   ```
   CALL SYSCS_UTIL.SYSCS_SET_DATABASE_PROPERTY('derby.user.rmlogin',
   'rmpassword');
   ```
5. Verlassen Sie ij und starten Sie den Derby Network Server.
6. Legen Sie im **UMS-Administrator** eine neue Datenquelle vom Typ `Derby` an mit dem Hostnamen des Derby-Servers und dem korrekten Serverport (Vorgabe ist `1527`), Benutzer `rmlogin` und Datenbank `rmdb`.

   Weitere Informationen zur Installation der Derby-Datenbank finden Sie unter http://db.apache.org/derby.

Lizenzierung der High Availability Erweiterung

Die Nutzung des HA-Netzwerks ist lizenzpflichtig. Die Basisinstallation enthält eine Lizenz für fünf in der UMS verwaltete Thin Clients, damit grundlegende Tests z. B. mit IGEL-Teststellungen möglich sind. Bitte kontaktieren Sie Ihren IGEL-Reseller, um Lizenzen für weitere Thin Clients zu erhalten.

- Registrieren Sie die erhaltene Lizenzdatei in der UMS-Konsole über **System→Lizenzen verwalten**.

  Der Lizenzstatus wird Ihnen im Administrationsbereich der Konsole angezeigt unter **Globale Konfiguration→Lizenz Konfiguration**.

17.2. IGEL Universal Customization Builder (UCB)

Mit dem Universal Customization Builder (UCB) lässt sich die Firmware von IGEL Universal Desktop Thin Clients bedarfsgerecht, sicher und einfach erweitern und anpassen. Installieren Sie beispielsweise lokale Gerätetreiber und Spezialanwendungen oder setzen Sie wichtige Windows Registry Keys – und das ohne tiefere Kenntnisse in Shell oder Windows-Scripting.

Der IGEL Universal Customization Builder (UCB) ist eine optionale Erweiterung (Extension) der IGEL Universal Management Suite (UMS), mit deren Hilfe sich individuelle Erweiterungspakete für die IGEL Universal Desktop-Firmware selbst erstellen, paketieren und zentral ausrollen lassen. Zahlreiche Hilfestellungen wie vordefinierte Templates, das benutzerfreundliche GUI oder der IGEL Helpdesk Support machen die Anwendung einfach und sicher. Der UCB unterstützt alle IGEL Universal Desktop Thin Clients

mit Linux und Windows Embedded – inklusive PCs und Thin Clients, die mithilfe der Migrationssoftware IGEL Universal Desktop Converter 2 (UDC2) standardisiert wurden.

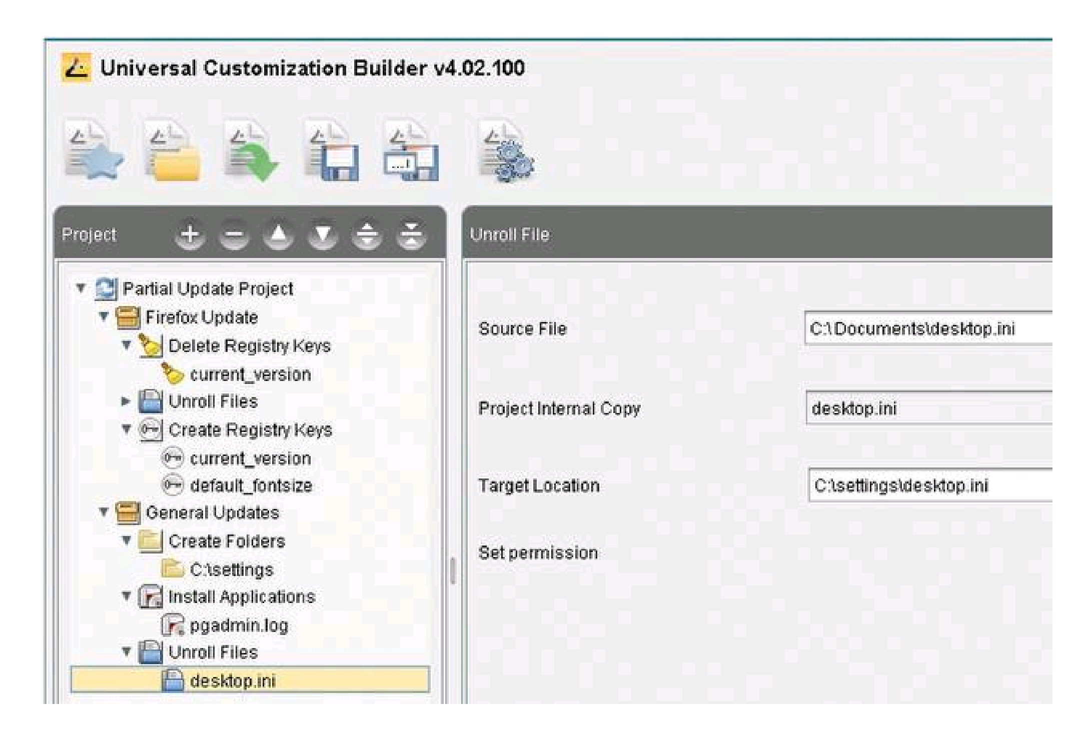


Abbildung 99: IGEL UCB

Typische Einsatzszenarien:

- Lokale Apps ergänzen: Anwendungen für den lokalen Betrieb zentral ausrollen, z.B. Kassensoftware für den Einzelhandel und andere branchenspezifische Software
- Gerätetreiber nachrüsten: für branchenspezifische Peripherie oder Originaltreiber
- Registry Keys setzen: Windows Embedded Standard individuell anpassen
- Kiosksysteme: Thin Clients mit besonderen lokalen Anwendungen oder Software-Clients ausstatten, um sie die unabhängig vom Firmennetzwerk zu betreiben, z.B. als Zeiterfassungsterminal

Features:

- Einfaches Erzeugen, Paketieren und Ausrollen von Firmware-Erweiterungspaketen für IGEL Linux (Custom Partition) und Windows Embedded Standard (Partial Update)
- Vordefinierte Templates: Task-orientiert für typische Anwendungsfälle
- Debugging: automatische Paketerzeugung mit syntaktische Überprüfung
- Automatische Versionierung innerhalb der Customization-Projekte
- Support der erstellten Pakete durch den IGEL Helpdesk

Vorteile:

- Projektkosten senken: mit dem UCB lassen sich Firmware-Erweiterungen jetzt einfach und schnell selbst vornehmen (ohne externen Dienstleister)
- Bedienkomfort: benutzerfreundliches GUI im gewohnten Look & Feel der IGEL UMS, keine tieferen Kenntnisse bzgl. Shell oder Windows-Scripting nötig (Templates)
- Schneller, kostengünstiger Roll-out: bequem und remote mittels IGEL UMS (im Lieferumfang aller IGEL Universal Desktop Thin Clients enthalten)
- Prozess- und Funktionssicherheit: Benutzerführung durch GUI und Templates, einfaches Debugging und Support von IGEL
- Transparenz: automatische Versionierung innerhalb der Customization-Projekte

Warnung: Testen Sie Partielle Updates oder Kundenspezifische Partitionen auf einem oder mehreren Thin Clients hinsichtlich der Funktionalität und Stabilität, bevor Sie Ihre Änderungen an produktive Systeme verteilen!

17.2.1. Voraussetzungen

IGEL Customization Builder ist Bestandteil der IGEL Universal Management Suite ab Version 4.03.200 (nur Windows). Es gelten jeweils die Systemvoraussetzungen der eingesetzten UMS-Version.

17.2.2. Lizenzierung

Die Nutzung der optionalen UCB-Erweiterung zur IGEL Universal Management Suite (UMS) erfordert eine UCB-Lizenz. Voraussetzung für den Erhalt einer dieser Lizenz ist die erfolgreiche Teilnahme an einem kostenpflichtigen IGEL UCB-Training (Inhouse- oder Classroom-Training).

Die Lizenz wird im Administrationsbereich der UMS Konsole registriert unter **Globale Konfiguration→Lizenzkonfiguration.**

17.2.3. Partielles Update für IGEL Thin Clients mit Windows Embedded Standard

Ein partielles Update ist eine Sammlung von Aufgaben, die in einem Skript zusammengefasst sind. Dieses Skript wird gemeinsam mit zu verteilenden Dateien an die Thin Clients gesendet. Das Skript wird auf dem Thin Client ausgeführt und arbeitet die vordefinierten Aufgaben ab.

Verschiedene Aufgaben wie die Verteilung von Dateien, das Anlegen von Registry Keys, das Ausführen von Befehlen und viele weitere können für ein Partielles Update definiert werden. Ähnliche Aufgaben vom gleichen Typ werden in Abschnitten zusammengefasst. Ein Projekt kann mehrere Partielle Updates mit verschiedenen Abschnitten und Aufgaben enthalten. Über die Importfunktion lassen sich mehrere Patielle Updates zu einem Projekt zusammenfassen.

Ein Beispiel sehen Sie hier:

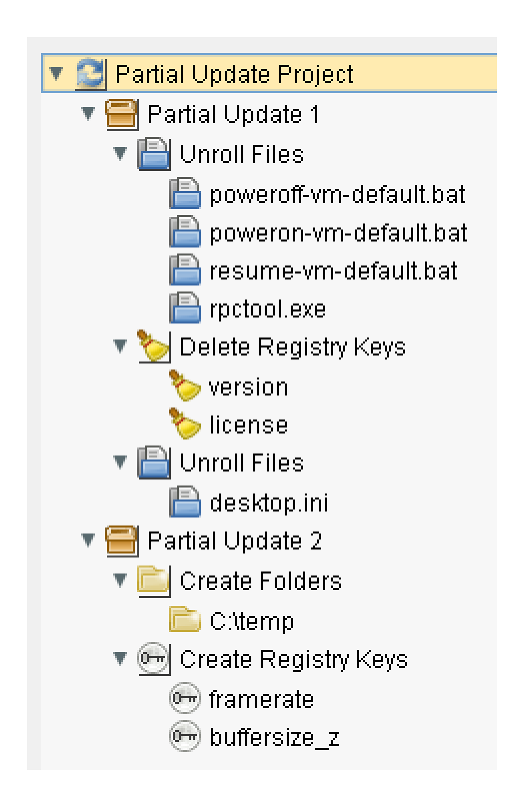


Abbildung 100: Partial Update Projekt

Folgende Typen von Aufgaben (Abschnitten) stehen in Projekten zur Verfügung:

- Datei ausrollen
- Verzeichnis erzeugen
- Rechte setzen
- Datei/Verzeichnis löschen
- Registry Key erzeugen
- Registry Datei ausrollen
- Registry Key löschen
- Anwendung installieren
- Kommando ausführen

Wird ein Projekt "gebaut", so werden alle notwendigen Skripte generiert und zusammen mit den benötigten Quelldateien in einem wählbaren Projektverzeichnis abgelegt.

Warnung: Testen Sie Partielle Updates oder Kundenspezifische Partitionen auf einem oder mehreren Thin Clients hinsichtlich der Funktionalität und Stabilität, bevor Sie Ihre Änderungen an produktive Systeme verteilen!

Projektfunktionen

Starten Sie den Universal Customization Builder in der UMS-Konsole über **System→Customization Builder öffnen**.

Folgende Funktionen sind für ein Partial Update Projekt verfügbar:



Neues Projekt erstellen (Strg+n)

1. Geöffnete Projekte werden gespeichert.
2. Der Anlagedialog öffnet sich.
3. Geben Sie einen **Projektnamen** ein.
4. Wählen Sie ein **Projektverzeichnis** für das Projekt; ein Unterordner mit dem Projektnamen wird darin angelegt, der alle Dateien des Projekts enthält.
5. Wählen Sie einen Projekttyp **Partial Update**.
6. Klicken Sie **OK**.



Projekt laden (Strg+o)

1. Geöffnete Projekte werden gespeichert.
2. Der Auswahldialog öffnet sich.

Wählen Sie eine Projektdatei aus (Partial Update Projekt `.ipu`).

1. Klicken Sie **Öffnen**.



Aktuelles Projekt speichern (Strg+s)

Speichert den aktuellen Zustand des Projekts im Projektverzeichnis.



Aktuelles Projekt speichern unter...

1. Der Anlagedialog öffnet sich.
2. Geben Sie einen **Projektnamen** ein.
3. Wählen Sie ein **Projektverzeichnis** für das Projekt; ein Unterordner mit dem Projektnamen wird darin angelegt, der alle Dateien des Projekts enthält.
4. Klicken Sie **OK**.

   Eine Kopie des aktuellen Projekts mit allen Dateien wird unter dem neuen Namen im gewählten Verzeichnis gespeichert.



Aktuelles Projekt schließen (Strg+0)

Das aktuelle Projekt wird gespeichert und geschlossen.



Projekt importieren (nur Partielles Update) (Strg+i)

1. Der Auswahldialog öffnet sich.
2. Wählen Sie eine Projektdatei aus (`.ipu`).
3. Klicken Sie **Öffnen**.

   Alle Elemente des gewählten Projekts werden dem aktuellen Projekt hinzugefügt.



Aktuelles Projekt bauen (Strg+b)

1. Der Auswahldialog öffnet sich.
2. Wählen Sie ein Zielverzeichnis für das Partielle Update.

   Warnung - alle Dateien im Zielverzeichnis werden gelöscht!

3. Klicken Sie **Öffnen**.

   Alle an den Thin Client zu sendenden Skripte und Dateien werden im Zielverzeichnis abgelegt. Nach dem erfolgreichen Abschluss des Prozesses enthält das Zielverzeichnis das fertige Partielle Update zur Verteilung an die Thin Clients.

Element hinzufügen (Einfügen)

- Legt abhängig vom aktuellen Elementtyp ein neues Element an.

Element löschen (Entfernen)

- Löscht die ausgewählten Elemente.

Element aufwärts verschieben (Bild auf)

- Verschiebt das ausgewählte Element um eine Position nach oben.

Element abwärts verschieben (Bild ab)

- Verschiebt das ausgewählte Element um eine Position nach unten.

Alle Elemente öffnen

- Öffnet alle Baumknoten.

Alle Elemente schließen

- Schließt alle Baumknoten.

Übertragung des Partiellen Updates

So spielen Sie Partielle Updates ins System ein:

1. Starten Sie die Thin Client Konfiguration (lokal oder in der UMS).
2. Wählen Sie **System→Updates→partielles Update**.
3. Aktivieren Sie die Checkbox **Partielles Update**.
4. Wählen Sie ein Übertragungsprotokoll (HTTP, FTP, FILE).
5. Geben Sie den Quellserver bzw. -pfad auf dem Laufwerk an (Zielverzeichnis des Partial Update Projekts).
6. Tragen Sie ggf. notwendige Anmeldedaten ein.
7. Klicken Sie **Übernehmen**, um die Einstellungen zu speichern.
8. Klicken Sie **Nach Updates suchen**, um die Quelle nach verfügbaren Updates zu durchsuchen (nur lokal am Thin Client).

Verfügbare Updates lassen sich dann direkt installieren. Das Gerät startet dazu neu. Auch nach Installation des Updates erfolgt ein Neustart.

In der UMS können Sie die Verteilung des Partiellen Updates über das Kontextmenü des Thin Clients starten (**Kommandos→WES→Partielles Update**) oder auch eine geplante Aufgabe dafür anlegen, um die Verteilung zeitgesteuert vorzunehmen.

17.2.4. Eigene Partition für Thin Clients mit IGEL Linux

Eine Custom Partition Projekt erstellt ein Archiv, welches auf Thin Clients mit IGEL Linux in eine Partition auf dem Datenträger umgewandelt wird. Die in diese Partition zu speichernden Dateien sind ebenfalls im Projektarchiv enthalten.

Ein Custom Partition Projekt besteht im Universal Customization Builder aus einem einzigen Knoten, die Erstellung einer Custom Partition erfolgt in wenigen Schritten:

1. Wählen Sie das Verzeichnis mit den zu übertragenden Dateien.
2. Starten Sie den Projektaufbau.
3. Wählen Sie den Pfad, auf dem die komprimierte Archivdatei gespeichert werden soll.

> **Warnung**: Testen Sie Partielle Updates oder Kundenspezifische Partitionen auf einem oder mehreren Thin Clients hinsichtlich der Funktionalität und Stabilität, bevor Sie Ihre Änderungen an produktive Systeme verteilen!

Projektfunktionen

Starten Sie den Universal Customization Builder in der UMS-Konsole über **System→Customization Builder öffnen**.

Folgende Funktionen sind für ein Custom Partition Projekt verfügbar:



Neues Projekt erstellen (Strg+n)

1. Geöffnete Projekte werden gespeichert.
2. Der Anlagedialog öffnet sich.
3. Geben Sie einen **Projektnamen** ein.
4. Wählen Sie ein **Projektverzeichnis** für das Projekt; ein Unterordner mit dem Projektnamen wird darin angelegt, der alle Dateien des Projekts enthält.
5. Wählen Sie den Projekttyp **Custom Partition**.
6. Klicken Sie **OK**.



Projekt laden (Strg+o)

1. Geöffnete Projekte werden gespeichert.
2. Der Auswahldialog öffnet sich.
3. Wählen Sie eine Projektdatei aus (Custom Partition Projekt `.icp`).
4. Klicken Sie **Öffnen**.



Aktuelles Projekt speichern (Strg+s)

➢ Speichert den aktuellen Zustand des Projekts im Projektverzeichnis.



Aktuelles Projekt speichern unter...

1. Der Anlagedialog öffnet sich.
2. Geben Sie einen **Projektnamen** ein.
3. Wählen Sie ein **Projektverzeichnis** für das Projekt; ein Unterordner mit dem Projektnamen wird darin angelegt, der alle Dateien des Projekts enthält.
4. Klicken Sie **OK**.

➢ Eine Kopie des aktuellen Projekts mit allen Dateien wird unter dem neuen Namen im gewählten Verzeichnis gespeichert.



Aktuelles Projekt schließen (Strg+0)

Das aktuelle Projekt wird gespeichert und geschlossen.



Aktuelles Projekt bauen (Strg+b)

1. Der Auswahldialog öffnet sich.
2. Wählen Sie ein Zielverzeichnis für die Custom Partition.

Warnung - alle Dateien im Zielverzeichnis werden gelöscht!

3. Klicken Sie **Öffnen**.

Alle an den Thin Client zu sendenden Skripte und Dateien werden im Zielverzeichnis abgelegt. Nach dem erfolgreichen Abschluss des Prozesses enthält das Zielverzeichnis die fertige Custom Partition zur Verteilung an die Thin Clients.

Übertragung der Kundeneigenen Partition

So spielen Sie Partielle Updates ins System ein:

1. Starten Sie die Thin Client Konfiguration (lokal oder in der UMS).
2. *Aktivieren* Sie die kundeneigene Partition und legen Sie die Partitionsgröße fest.
3. Definieren Sie das Zielverzeichnis des Projekts als *Downloadquelle* der Partition.
4. Definieren Sie ggf. beim Ein- oder Aushägen der Partition auszuführende *Aktionen*.
5. Lassen Sie die Einstellungen für den Thin Client wirksam werden.

Partition aktivieren

Standardmäßig ist die Kundenpartition nicht aktiv.

➢ Klicken Sie im Setup **System→Firmwareanpassung→Eigene Kundenpartition→Partition**, um die Kundenpartition im IGEL Setup des Thin Clients (oder auch mit IGEL Universal Management Suite) über den Setuppfad zu aktivieren.

Die Größe der Partition wird über einen nummerischen Wert (Byte) in Verbindung mit einer multiplikativen Endung angegeben.

Sinnvolle Größenangaben sind z. B. 100 K (für 100 KiB = 100 * 1024 Byte) oder 100 M (für 100 MiB = 100 * 1024 * 1024 Byte).

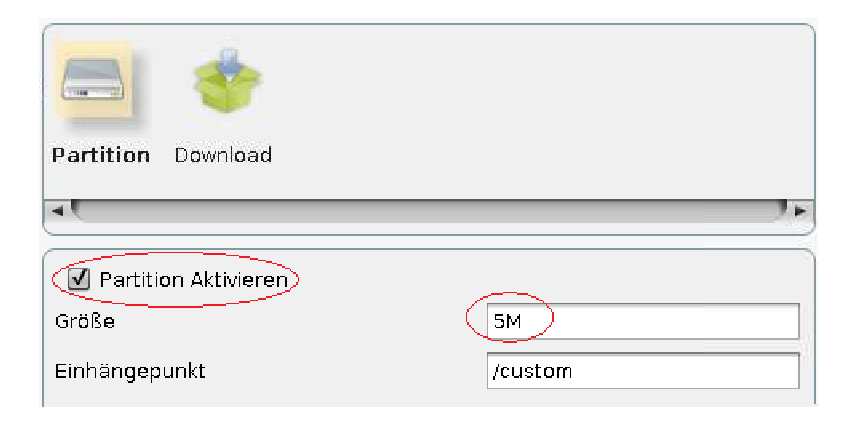


Abbildung 101: kundenspezifische Partition aktivieren

Für die Größe der Partition sollten mindestens 100 KiB gewählt werden, maximal sollten nicht mehr als 300 MiB durch die kundenspezifische Partition reserviert werden (bezogen auf die 1 GB Standard-CF der IGEL Linux Thin Clients), da spätere Firmwareupdates unter Umständen mehr Speicherplatz benötigen als die aktuelle Version.



Abbildung 102: Systemrückmeldung

➢ Klicken Sie **Übernehmen** oder **OK**, um die Einstellungen zu bestätigen.

  Die Partition wird erstellt und am definierten Punkt eingehängt.

Ein Statusfenster informiert über den Prozess bzw. Fehler beim Anlegen der Partition. Ist z. B. auf dem Speichermedium nicht genügend freier Platz vorhanden, kann die Partition nicht erstellt werden.

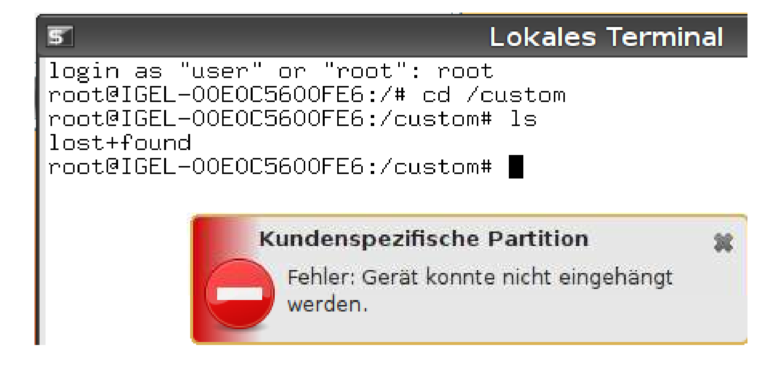


Abbildung 103: Fehlermeldung

Die Änderung der Größe einer bereits zuvor angelegten Kundenpartition kann auch durch einen Prozess verhindert sein, der noch auf diese Partition zugreift – etwa wenn im Terminalfenster noch deren Inhalt angezeigt wird.

Downloadquelle definieren

Um Daten in die Kundenpartition zu laden, muss im Bereich Download mindestens eine Quelle für Partitionsdaten angelegt werden.

➢ Klicken Sie **Hinzufügen**.

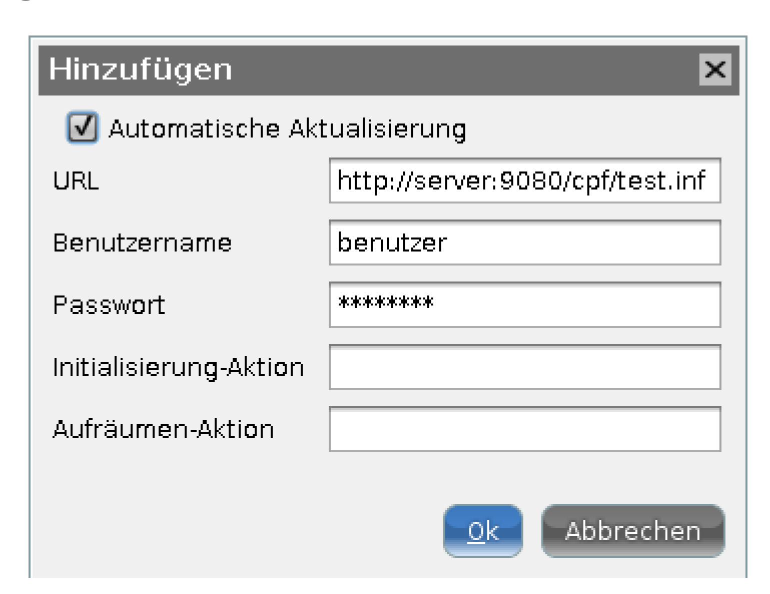


Abbildung 104: Downloadquelle definieren

Für die Übertragung stehen die gleichen Protokolle zur Verfügung wie auch im Firmwareupdate, z. B. HTTP, HTTPS, FTP. Als Ziel muss eine `INF`-Datei angegeben werden, welche wiederum ein mit bzip2 gepacktes tar-Archiv referenziert.

Die Struktur der INF-Datei ist dabei wie folgt:

`[INFO], [PART]`	Headerinformationen
`file="test.tar.bz2"`	Gepacktes tar-Archiv
`version="1"`	Version der Datei

Die zu übertragenden Dateien müssen also zunächst in ein `tar`-Archiv gepackt werden, welches anschließend mit `bzip2` komprimiert wird. Diese Datei wird in der INF-Datei referenziert, welche das Ziel der URL darstellt.

Das `tar`-Archiv kann unter Windows z. B. mit dem Opensource-Programm 7-Zip (www.7-zip.org) erfolgen, dieses Programm erlaubt auch die Komprimierung als `bzip2`. Unter Linux ist die Erstellung von `tar`- und `bz2`-Dateien oft mit Bordmitteln möglich.

Dieses Verfahren erlaubt es, die Datei(en) auf dem Server durch eine aktuelle Version zu ersetzen, sodass der Thin Client beim nächsten Bootvorgang diese nachlädt. Dazu muss in der `INF`-Datei der Parameter `Version` erhöht werden.

Aktionen ausführen

Im Anschluss an das Einhängen bzw. Aushängen der Kundenpartition können automatisch Kommandos (Shellscript) ausgeführt werden. Z. B. kann ein in die Partition herunter geladenes Programm gestartet bzw. beim Herunterfahren (dabei wird die Partition wieder abgehängt) beendet werden.

18. Glossar

Active Directory (AD)

Active Directory (AD) ist eine Implementation der LDAP-Verzeichnisdienste von Microsoft für Windows Umgebungen. Active Directory erlaubt Administratoren die Zuweisung von unternehmensweiten Regeln, die Verteilung von Software an Windowsrechner sowie die Installation wichtiger Systemupdates in der kompletten IT-Infrastruktur. Alle Daten und Einstellungen einer Organisation des Active Directory werden in einer zentralen Datenbank gespeichert. Die Organisation eines Active Directory kann von einigen Hundert bis mehrere Millionen Objekte umfassen.

Lightweight Directory Access Protocol (LDAP)

Lightweight Directory Access Protocol (LDAP) ist ein Netzwerkprotokoll für die Abfrage oder Modifikation von Verzeichnisdiensten über TCP/IP. Ein Verzeichnis ist ein Satz aus Informationen mit ähnlichen Attributen, organisiert in einer logischen sowie hierarchischen Struktur – ein bekanntes Beispiel ist ein Telefonverzeichnis, welches sich aus einer alphabetisch sortierten Namensliste mit angefügten Telefonnummern und Adressen zusammensetzt.

19. Index

A

Active Directory (AD) 162

Active Directory / LDAP einbinden 122

Active Directory anbinden 73

Active Directory Benutzer importieren 127

Administration 139

Administrationsbereich 117

Administrative Aufgaben erstellen 119

Administratoren und Gruppen 131

Administratorkonten und Zugriffsrechte 131

Aktionen ausführen 162

Aktive Embedded-DB optimieren 45

Allgemeine Administratorenrechte 134

Anbindung externer Datenbanksysteme....17, 150

Anmerkungen 142

Apache Derby 18, 152

Arbeiten mit IGEL UMS.....................................28

Aus dem UMS WebDAV importieren 114

B

Backup auf der Kommandozeile........................44

Backup erstellen 43

Backup löschen 43

Backup wiederherstellen...................................43

Bearbeiten 30

Bedingungen festlegen......................................49

Beispiel View erstellen......................................97

Beispiele 51

Benutzerprofil zuweisen....................................74

Benutzerprofile - IGEL Shared Workplace 71

Benutzerprotokolle...139

C

Cache-Konfiguration..123

Caches erneuern...121

D

Das Konsolenfenster.. 28

Datei am UMS Server registrieren 109

Datei auf den UMS Server übertragen 111

Datei vom Thin Client entfernen 111

Datei zum Thin Client übertragen................... 110

Dateien 109

Datenbanksysteme (DBMS)............................ 147

Datenquelle aktivieren 45

Datenquelle anlegen.. 44

Datenquelle kopieren 45

Datenquellen 44

Datensicherungen.. 43

Der IGEL UMS-Administrator............................ 39

Details 105

Dialogfenster Logging 140

Downloadquelle definieren 161

E

Eigene Partition für Thin Clients mit IGEL Linux 158

Eigenschaften der IGEL UMS 9

Einfache Hochverfügbarkeit 144

Einrichtung und Verwendung........................... 72

E-Mail-Einstellungen...................................... 125

Ergebnisliste des Imports 130

Ergebnisse... 107

Erste Schritte 19

Erster Server des HA-Netzwerks..................... 148

Export der View-Ergebnisse via Mail 121

Externe VNC-Viewer 54

Extras 31

F

Filter einstellen 140

Filter für Ereignisse einstellen 141

Filter für Kategorien einstellen 142

Filter für Nachrichten..................................... 141

Firmware Lizenzen 59

G
Geplante Aufgaben.......................................103
Geplantes Backup (Embedded-DB) erstellen ...119
Gerätespezifische Einstellungen UD W7 78
Gerätespezifische Parameter UD Linux 77
Globale Konfiguration......................................119
Grundlagen und Voraussetzungen 55
Grundlegende Berechtigungen 133

H
HA_Installation 146
Hilfe 31
Hochverfügbarkeit und Lastverteilung............145

I
IGEL Shared Workplace am Thin Client aktivieren 74
IGEL UMS High Availability (HA) 143
IGEL Universal Customization Builder (UCB) 152
IGEL Universal Management Suite 8
IGEL VNC-Viewer 53
Im Benutzerprofil konfigurierbare Parameter....77
Import mit IGEL Seriennummer 26
Import mit kurzem Format................................24
Import mit langem Format................................25
Inhaltsbereich 35
Installation 12
Installation der einfachen Hochverfügbarkeitslösung..............................147
Installation eines UMS-Servers..........................13
Installation einzelner HA-Netzwerkkomponenten 149
Installation UMS-Konsole 147
Installation UMS-Server - auch einzelne HA-Netzwerkkomponenten............................147
Installation von Serverzertifikaten 116
Installationsvoraussetzungen....................12, 147

K
Kommandos für Aufgaben...............................104
Komponenten der IGEL UMS............................10
Konfiguration in der UMS-Konsole 73
Konfigurationsoptionen.................................. 144
Konsolenzertifikat importieren....................... 117
Kontextmenü 37

L
Lightweight Directory Access Protocol (LDAP) 162
Lizenzierung 154
Lizenzierung der High Availability Erweiterung 152
Lizenzkonfiguration 123
Lizenzverwaltung 59
Logdateien und Support 143
Logging... 124
Logging Informationen löschen 121
Log-in des Benutzers.. 75
Log-out und Benutzerwechsel 77
Löschen von Objekten in der UMS / Papierkorb 38

M
Masterprofile 78
Masterprofile aktivieren 79
Menüzeile 29
Microsoft SQL Server 17, 150

N
Nachrichten 35
Navigationsbaum (Management Tree)............. 33
Neue Aufgabe anlegen 103
Neue View erstellen.. 96
Neues Profil - Optionen 65

O
Objektbezogene Zugriffsrechte 135
Optionale Erweiterungen (HA und UCB) 143
Oracle...17, 150

P
Partielles Update für IGEL Thin Clients mit Windows Embedded Standard 154
Partition aktivieren 159
Ports/Zeitlimits 40

PostgreSQL..18, 151
Profil und Firmwareinformationen exportieren.66
Profil und Firmwareinformationen importieren 67
Profile 62
Profile erstellen 65
Profile exportieren und importieren 66
Profile löschen 71
Profile mit unbekannter Firmware importieren.67
Profile überprüfen 70
Profile verwenden...64
Profile zuweisen 69
Profileinstellungen konfigurieren.......................68
Profilzuweisung vom Thin Client entfernen 70
Projektfunktionen...................................156, 158

R

Rangfolge der Einstellungen..............................63
Rangfolge der Profile 63, 75, 80
Regeln für Vorgabeverzeichnisse definieren......49

S

Schlüssel und Werte im Profil erstellen.............89
Servereinstellungen..40
Servereinstellungen ändern 112
Sicheres Spiegeln (VNC mit SSL) 55
Sitzungen überschreiben...................................69
Snapshot-Dateiquellen 42
Sonderfall Strukturtag 52
Spiegeln (VNC) 53
Statuszeile..36
Suche im Active Directory 129
Suche nach Objekten in der UMS......................37
Symbolerklärung...129
Symbolleiste 32
System 29

T

Templateprofile 83
Templateprofile aktivieren 85
Templateprofile und Werte den Thin Clients zuordnen.. 92
Templateschlüssel in Profilen verwenden......... 91
Templateschlüssel und Werte erstellen 86
Thin Clients 30, 46
Thin Clients am UMS Server registrieren........... 21
Thin Clients automatisch registrieren................ 27
Thin Clients im Netzwerk suchen 21
Thin Clients importieren 24
Thin Clients konfigurieren 52
Thin Clients löschen...................................... 121
Thin Clients manuell erstellen 27
Thin Clients manuell registrieren...................... 26
Thin Clients registrieren................................... 23
Thin Clients scannen 22
Thin Clients sicher spiegeln 57
Thin Clients verschieben.................................. 48
Thin Clients verwalten 46
Typische Einsatzbereiche...................................8

U

Über dieses Dokument 5
Übertragung der Kundeneigenen Partition 159
Übertragung des Partiellen Updates 157
Übertragung ohne Zuweisung 111
UDC2-Lizenzen verteilen.................................. 60
UDC2-Testlizenzen.. 59
UMS Administration 35
UMS Netzwerk 117
UMS-Administrator – Das Verwaltungsprogramm 11
UMS-Installation aktualisieren 15
UMS-Konsole – Die zentrale Schaltstelle........... 11
UMS-Konsole mit Server verbinden 19
UMS-Server... 118
UMS-Server – Das Back-End 10
Unbenutzte Firmware entfernen.................... 120
Universal Firmware Update.....................112, 123

Unter LINUX aktualisieren 16
Unter LINUX installieren 14
Unter WINDOWS aktualisieren 15
Unter WINDOWS installieren 13
Update einem Thin Client zuweisen 115
Update suchen und herunterladen 113
Upgrade von Lizenzen 61

V

Verfügbare Rechte 137
Verzeichnis erstellen 46
Verzeichnis importieren 47
Verzeichnis löschen 48
Verzeichnisregel anwenden 50
Verzeichnisregel erstellen/bearbeiten 49
View Ergebnisliste speichern 101
View per E-Mail verschicken 102
Views 96
VNC-Logging 58
VNC-Sitzung starten 53
Von lokaler Quelle importieren 114
Voraussetzungen 154

W

Wake-on-LAN-Konfiguration 124
Was ist neu in 4.09.100? 6
Weitere Einstellungen 42
Weitere Server 148
Wertesammlungen 93
Wichtige Informationen 2

Z

Zeitgesteuertes Backup 44
Zeitplan 106
Zertifikat entfernen 116
Zertifikat speichern 116
Zertifikate 45
Zertifikate verwalten 116
Zugeordnete Objekte 36
Zugriffsrechte 132
Zugriffsrechte im Administrationsbereich 138
Zuordnung 107
Zusätzliche Einstellungen 126